www.rockwellautomation.com

Oficinas corporativas de soluciones de potencia, control e información

Américas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europa/Medio Oriente/África: Rockwell Automation, Vorstlaan/Boulevard du Souverain 36, 1170 Bruselas, Bélgica, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia-Pacífico: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Argentina: Rockwell Automation S.A., Alem 1050, 5º Piso, CP 1001AAS, Capital Federal, Buenos Aires, Tel.: (54) 11.5554.4000, Fax: (54) 11.5554.4040, www.rockwellautomation.com.ar
Chile: Rockwell Automation Chile S.A., Luis Thayer Ojeda 166, Piso 6, Providencia, Santiago, Tel.: (56) 2.290.0700, Fax: (56) 2.290.0707, www.rockwellautomation.cl
Colombia: Rockwell Automation S.A., Edf. North Point, Carrera 7 N° 156 – 78 Piso 18, PBX: (57) 1.649.96.00 Fax: (57)649.96.15, www.rockwellautomation.com.co
España: Rockwell Automation S.A., Doctor Trueta 113-119, 08005 Barcelona, Tel.: (34) 932.959.000, Fax: (34) 932.959.001, www.rockwellautomation.es
México: Rockwell Automation S.A. de C.V., Bosques de Ciérulos Nº 160, Col. Bosques de Las Lomas, C.P. 11700 México, D.F., Tel.: (52) 55.5246.2000, Fax: (52) 55.5251.1169, www.rockwellautomation.com.mx
Perú: Rockwell Automation S.A., Av Victor Andrés Belaunde N°147, Torre 12, Of. 102 – San Isidro Lima, Perú, Tel: (511) 441.59.00, Fax: (511) 222.29.87, www.rockwellautomation.com.pe
Puerto Rico: Rockwell Automation Inc., Calle 1, Metro Office # 6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, Fax: (1) 787.706.3939, www.rockwellautomation.com.pr
Venezuela: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, Fax: (58) 212.943.3955, www.rockwellautomation.com.ve

Publicación: SAFEBK-RM002A-ES-P – Febrero de 2009

SAFEBOOK 3 – Sistemas de seguridad para maquinaria industrial/principios, estándares e implementación

SAFEBOOK 3

LISTEN. THINK. SOLVE.SM

Allen-Bradley
GuardMaster®

Sistemas de seguridad para maquinaria industrial

Principios, estándares e implementación

Rockwell Automation

Contenido

Directivas y legislación de la Unión Europea

Esta sección se proporciona como guía para las personas encargadas de la seguridad de las máquinas, especialmente sistemas protectores de guarda y sistemas de protección en la Unión Europea. Ha sido concebida para diseñadores y usuarios de equipo industrial.

Con el objeto de promover el concepto de un mercado abierto dentro del Área Económica Europea (EEA) (que comprende todos los estados miembros de la UE y 3 países adicionales) todos los estados miembros están obligados a promulgar legislación que defina los requisitos de seguridad esenciales para las maquinarias y su uso.

Las máquinas que no cumplan estos requisitos no podrán suministrase dentro de los países de la EEA.

Hay varias directivas europeas que pueden aplicarse a la seguridad de máquinas y equipos industriales, pero las dos que tienen la relevancia más directa son:

1 La Directiva de máquinas

2 La Directiva de uso de equipo de trabajo por trabajadores en el ámbito laboral

Estas dos directivas están directamente relacionadas con los Requisitos de Salud y Seguridad Esenciales (EHSR) de la directiva de máquinas y pueden usarse para confirmar la seguridad del equipo indicada en la Directiva de uso de equipo de trabajo.

Esta sección trata aspectos de ambas directivas y se recomienda enfáticamente que las personas relacionadas con el diseño, suministro, compra o uso de equipo industrial dentro de la EEA y también algunos otros países europeos se familiaricen con sus requisitos. La mayoría de suministradores y usuarios de maquinaria simplemente no podrán suministrar ni operar maquinaria en estos países a menos que cumplan con estas directivas.

Existen otras directivas europeas pertinentes a la seguridad industrial. La mayoría son especializadas en su aplicación y por lo tanto no se incluyen en esta sección, pero es importante anotar que, cuando sea pertinente, sus requisitos también deben cumplirse. Algunos ejemplos son: La Directiva de baja tensión y la Directiva ATEX.

La Directiva de máquinas

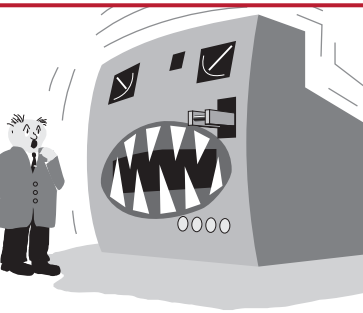
Esta Directiva (98/37/EC) abarca el suministro de nueva maquinaria y otros equipos, inclusive componentes de seguridad. Es una negligencia suministrar maquinaria a menos que cumpla con la Directiva. Esto significa que la maquinaria deberá satisfacer una amplia gama de EHSR contenidos en el Anexo I de la Directiva, deberá realizarse una evaluación de conformidad, y deberá otorgarse una “Declaración de conformidad”, y deberá incluir el distintivo CE.

Distintivo CE colocado en la máquina

Las disposiciones clave de la Directiva entran en vigencia para la maquinaria el 1 de enero de 1995, y para los componentes de seguridad el 1 de enero de 1997. Se otorgó un período de transición de dos años en el cual podían seguirse las regulaciones nacionales existentes o la nueva Directiva. Es responsabilidad del fabricante, importador o suministrador final del equipo asegurarse de que el equipo suministrado cumpla con la Directiva.

Una nueva versión de la Directiva para máquinas se publicó como 2006/42/EC en 2006. La nueva Directiva no reemplazará las disposiciones de la Directiva existente hasta fines de 2009. Mientras tanto, estará vigente la Directiva para máquinas existente. El siguiente texto corresponde a la Directiva 98/37/EC existente, pero los cambios serán mínimos en términos de los requisitos esenciales para la mayoría de tipos de maquinaria en la nueva Directiva.

Requisitos esenciales de salud y seguridad



La máquina debe cumplir con EHSRs

La Directiva proporciona una lista de Requisitos de salud y seguridad esenciales (conocidos como EHSR) con los cuales debe cumplir la maquinaria cuando sea pertinente. El propósito de esta lista es asegurar que la maquinaria es segura y que está diseñada y construida de manera que pueda usarse, ajustarse y mantenerse en todas las fases de su vida útil sin poner en riesgo a los operadores.

La directiva también proporciona una jerarquía de medidas para eliminar los riesgos:

(1) Diseño de seguridad inherente – En la medida de lo posible, el diseño mismo evitará cualquier riesgo.

En los casos en que esto no sea posible, deberán usarse **(2) dispositivos de protección adicionales**, por ej., guardas con puntos de acceso enclavados, barreras inmateriales tales como cortinas de luz, alfombras de seguridad, etc.

Cualquier otro riesgo que no pueda eliminarse mediante los métodos anteriores deberá eliminarse mediante **(3) equipo de protección personal y/o formación técnica**. El suministrador de la máquina deberá especificar lo apropiado.

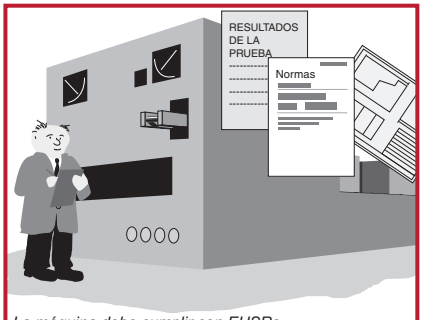
Deberá usarse materiales idóneos para construcción y operación. Deberá proporcionarse iluminación e instalaciones de manejo adecuadas. Los controles y los sistemas de control deben ser seguros y fiables. Las máquinas no deben ponerse en marcha de forma intempestiva y deben tener uno o más dispositivos de paro de emergencia acoplados. Se deberá dar consideración a instalaciones complejas donde los procesos corriente arriba o corriente abajo puedan afectar la seguridad de una máquina. El fallo de una fuente de alimentación eléctrica o circuito de control no deberá causar una situación peligrosa. Las máquinas deben ser estables y capaces de soportar tensiones previsibles. No deben tener bordes ni superficies expuestas que puedan causar lesiones al personal.

Deberán usarse guardas o dispositivos de protección para evitar riesgos tales como los causados por piezas móviles. Estos deben ser de construcción robusta y difíciles de anular. Las guardas fijas deben ser sólo del tipo que requiere montaje y desmontaje mediante el uso de herramientas. Las guardas móviles deben estar enclavadas. Las guardas ajustables deben tener la capacidad de ser ajustadas de inmediato, sin el uso de herramientas.

Deberán evitarse los peligros eléctricos y de suministro de energía. Deberá haber riesgo mínimo de lesión causada por temperatura, explosión, ruido, vibración, polvo, gases o radiación. Deberán tomarse las provisiones apropiadas al realizar el mantenimiento y servicio. Deben proporcionarse indicaciones y dispositivos de advertencia suficientes. La maquinaria debe proporcionarse con instrucciones para realizar la instalación, uso, ajuste, etc. con toda seguridad.

Evaluación de conformidad

El diseñador u otra persona responsable deberá mostrar pruebas que verifiquen la conformidad con los EHSR. Este archivo debe incluir toda la información pertinente tales como resultados de pruebas, dibujos, especificaciones, etc.



La máquina debe cumplir con EHSRs

Un Estándar Europeo Armonizado (EN) listado en el Official Journal (OJ) de la Unión Europea bajo la Directiva para maquinarias, y cuya fecha de suspensión de presunción de conformidad no ha caducado, otorga una presunción de conformidad con algunos de los EHSR. (Muchos estándares recientes listados en el OJ incluyen una referencia cruzada que identifica los EHSR cubiertos por el estándar).

Por lo tanto, cuando el equipo cumple con dichos estándares europeos armonizados actuales, la tarea de demostrar conformidad con los EHSR queda considerablemente simplificada, y el fabricante también se beneficia de la mayor certeza legal. Estos estándares no son un requisito legal, sin embargo, su uso se recomienda enfáticamente ya que probar la conformidad por métodos alternativos puede ser extremadamente complejo. Estos estándares apoyan la Directiva de maquinarias y son producidos por CEN (el Comité Europeo de Estandarización) en cooperación con ISO y CENELEC (el Comité Europeo de Estandarización Electrotécnica) en cooperación con IEC.

Deberá realizarse una evaluación de riesgos detallada y documentada para asegurar que se han eliminado todos los posibles riesgos de la máquina. De manera similar, es responsabilidad del fabricante de la máquina asegurar que se cumplan todos los EHSR, inclusive aquellos no tratados por los Estándares EN armonizados.

Expediente técnico

La persona responsable de la declaración de conformidad debe asegurarse de que la siguiente documentación estará disponible en las instalaciones para fines de inspección.

Un expediente técnico que incluya:

1. Esquemas generales del equipo, incluyendo dibujos del circuito de control.

2. Esquemas detallados, notas de cálculo, etc., requeridos para verificar la conformidad de la maquinaria con los EHSR.

3. Una lista de:
   - Los EHSR pertinentes al equipo.
   - Los Estándares Europeos Armonizados aplicables.
   - Otros estándares aplicables.
   - Especificaciones técnicas de diseño.

4. Una descripción de los métodos adoptados para eliminar los riesgos que presenta la máquina.

5. Si lo desea, cualquier informe técnico o certificado obtenido de un organismo (entidad de pruebas) o laboratorio aprobado.

6. Si se declara la conformidad con un Estándar Europeo Armonizado, cualquier informe técnico que proporcione los resultados de las pruebas correspondientes.

7. Una copia de las instrucciones de la máquina.

En el caso de fabricación en serie, detalles de las medidas internas (sistemas de calidad, por ejemplo) para asegurar que toda la maquinaria producida está en conformidad:

- El fabricante debe realizar la investigación o pruebas necesarias de los componentes, conexiones o la maquinaria completa para determinar si por su diseño y construcción puede instalarse y ponerse en servicio con toda seguridad.

- El expediente técnico no necesita existir como archivo único permanente, pero debe ser posible archivarlo para que esté disponible en un plazo razonable. Deberá estar disponible durante diez años después de la producción de la última unidad. El hecho de que no esté disponible como respuesta a una petición justificada de una autoridad de aplicación de leyes puede ser motivo para dudar la conformidad.

El expediente técnico no necesita incluir planes detallados ni otra información específica respecto a los submontajes usados para la fabricación de la máquina, a menos que estos sean esenciales para verificar la conformidad con los EHSR.

Evaluación de conformidad para máquinas listadas en el Anexo IV

Evaluaciones de conformidad

Algunos tipos de equipo están sujetos a medidas especiales. Estos equipos aparecen listados en el Anexo IV de la Directiva e incluyen máquinas peligrosas tales como máquinas para trabajo de madera, prensas, máquinas de moldeado por inyección, equipo subterráneo, mecanismos de elevación para mantenimiento de vehículos, etc.

El Anexo IV también incluye ciertos componentes de seguridad tales como cortinas de luz y unidades de control bimanual.

Para las máquinas listadas en el Anexo IV que cumplen con los Estándares Europeos Armonizados, se puede seleccionar entre tres procedimientos:

1. Enviar el expediente técnico a una entidad notificada que confirmará recepción del archivo y se quedará con él. *Nota*: *Con esta opción no hay evaluación del archivo. Puede usarse como referencia posteriormente en el caso de que ocurra un problema o una declaración de falta de conformidad.*

2. Enviar el expediente técnico a una entidad notificada que verificará que se hayan aplicado correctamente los Estándares Armonizados y emitirá un certificado de suficiencia para el archivo.

3. Remitir una maquinaria de muestra a una entidad notificada (agencia de pruebas) para examen de tipo CE. Si pasa el examen, se otorgará un certificado de examen de tipo CE para la máquina.


Exámenes de entidad de notificación

En el caso de máquinas listadas en el Anexo IV que no cumplen con un estándar o para las cuales no existe un Estándar Europeo Armonizado, deberá remitirse una muestra de la maquinaria a una entidad notificada (institución de pruebas) para el examen de tipo CE.

Entidades notificadas

Se ha constituido una red de entidades notificadas que se comunican entre sí y trabajan siguiendo criterios comunes en toda la EEA y

algunos otros países. Las entidades notificadas son asignadas por los gobiernos (no por el sector) y los detalles de las organizaciones con estado de entidades notificadas puede obtenerse en:

http://europa.eu.int/comm/enterprise/newapproach/legislation/nb/en 98-37-ec.pdf.

Examen CE de tipo

Para el examen tipo CE, la entidad notificada requerirá un archivo técnico y acceso a la máquina a ser examinada. Verificarán que la máquina esté fabricada en conformidad con su archivo técnico y que satisface los EHSR aplicables. Si pasa el examen, se emitirá un certificado de examen de tipo CE. Una entidad que se rehuse a emitir un certificado deberá informar los casos a las otras entidades notificadas.

Procedimiento de la Declaración CE de conformidad

CE La persona responsable emitirá una Declaración de Conformidad CE y colocará el distintivo CE sobre todas las máquinas suministradas. Las máquinas también deberán suministrarse con la Declaración de Conformidad CE.

Nota: Los componentes de seguridad deben tener una Declaración de Conformidad CE pero no el distintivo CE con respecto a la Directiva de maquinarias (aunque pueden tener el marcado CE para indicar conformidad con otras directivas, tales como las Directivas EMC y/o de baja tensión).

El distintivo CE indica que la máquina cumple con todas las Directivas Europeas aplicables y que se han realizado los procedimientos apropiados de evaluación de conformidad. Es un delito aplicar el distintivo CE para la Directiva de maquinarias a menos que la máquina cumpla con los EHSR para todas las directivas aplicables y tenga todas medidas de seguridad correspondientes. Es también un delito colocar un distintivo que pueda confundirse con el marcado CE.

Declaración de incorporación de CE

Cuando el equipo se suministra para ensamblaje con otros componentes para formar una máquina completa posteriormente, la persona responsable debe emitir una DECLARACIÓN DE INCORPORACIÓN con éste (en lugar de una declaración de conformidad). El marcado CE NO debe usarse. La declaración debe indicar que el equipo no debe ponerse en servicio hasta que se haya declarado la conformidad de la máquina en la cual ha sido incorporado.

Esta opción no está disponible para equipos que pueden funcionar independientemente o que modifican la función de una máquina.

Maykit Wright Ltd.
Declaración de conformidad

Respecto a las siguientes directivas:

Directiva europea sobre maquinarias 98/37/EC;
(Cualquier otra directiva referente a la maquinaria, por ej., la directiva de EMC, también debería incluirse aquí.)

Compañía:

Maykit Wright Ltd.
Main Street
Anytown Industrial Estate
Anytown, England AB1 2DC
Tel: 00034 000890. Fax: 00034

Máquina: Máquina empaquetadora de carnes
Tipo: Vacustarwrap 7D
Número de serie: 00516

Conforme a estándares: *(Todos los estándares armonizados europeos vigentes y, si corresponde, toda norma y especificaciones nacionales.)*

Si el Anexo IV abarca esta máquina, sería necesario incluir en este punto uno de los siguientes:

– El nombre y dirección de la entidad aprobada y el número de Certificado de examen de tipo, o bien

– El nombre y dirección de la entidad aprobada que emitió un Certificado de suficiencia para el archivo técnico

– El nombre y dirección de la entidad aprobada a la cual se envió el archivo técnico.

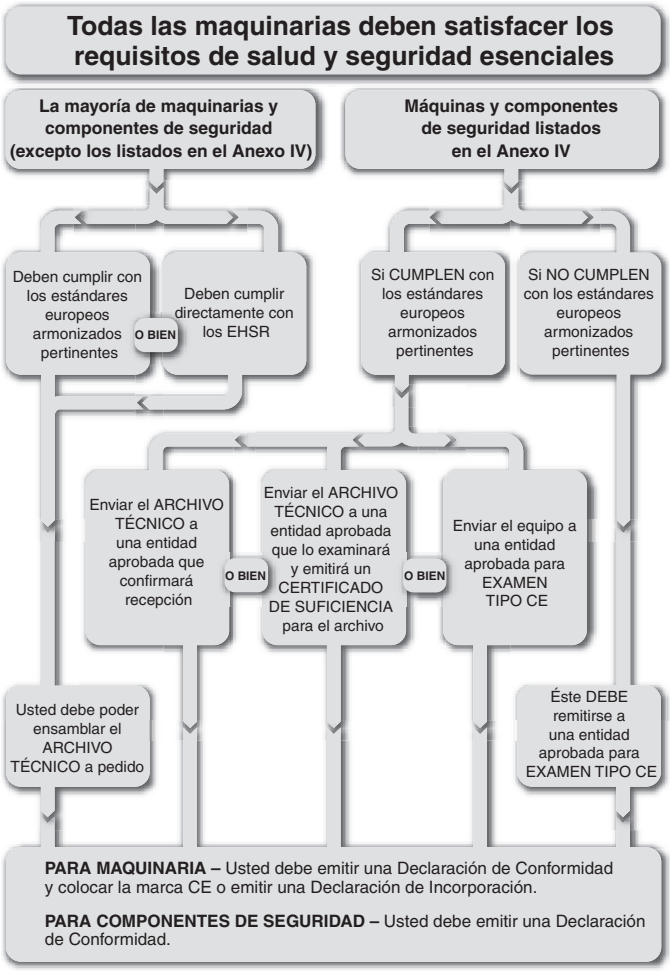
Con ello se declara que la máquina indicada anteriormente cumple con los requisitos esenciales de salud y seguridad de la Directiva europea sobre maquinarias 98/37/EC.

G. V. Wright

G.V. Wright, Director Administrativo
Emitido el 17 de enero de 2003

Ejemplo de una Declaración de conformidad para una máquina que tiene autocertificación

Directiva de uso de equipo de trabajo



Descripción general de procedimientos para la Directiva de Maquinarias

Mientras que la Directiva para máquinas está dirigida a los proveedores, esta Directiva (89/655/EEC según modificación por 95/63/EC y 2001/45/EC) está dirigida a los usuarios de la maquinaria. Abarca todos los sectores industriales e imponen deberes generales a los usuarios junto con requisitos mínimos para la seguridad del equipo de trabajo. Todos los países de la EEA están promulgando sus propias formas de legislación para implementar esta Directiva.

Es más fácil entender el significado de los requisitos de la Directiva de uso de equipo de trabajo si se examina el ejemplo de su implementación en la legislación nacional. Examinaremos su implementación en el Reino Unido bajo el nombre Regulaciones sobre disposición y uso de equipo de trabajo (conocidos generalmente con la abreviatura P.U.W.E.R.). La forma de implementación puede variar de un país a otro, pero el efecto de la Directiva es el mismo.

Regulaciones 1 a 10

Estas regulaciones proporcionan detalles de qué tipos de equipo y lugares de trabajo están cubiertos por la Directiva.

También imponen deberes generales a los usuarios, tales como implementar sistemas seguros de trabajo y proporcionar equipos idóneos y seguros los cuales deben recibir el mantenimiento adecuado. Los operadores de las máquinas deben recibir información y formación técnica adecuadas para que puedan usar la máquina con toda seguridad.

Las máquinas nuevas (y la maquinaria de segunda mano proveniente de países fuera de la EEA) suministradas después del 1 de enero de 1993, deben satisfacer las directivas pertinentes, por ej., la Directiva de Maquinarias (sujeto a arreglos de transición). Los equipos de segunda mano provenientes de países de la EEA que se suministraron por primera vez en el lugar de trabajo deben satisfacer inmediatamente las regulaciones 11 a 24.

Nota: La maquinaria existente o de segunda mano que sea significativamente reacondicionada o modificada se clasificará como equipo nuevo, de manera que el trabajo que se realice en la misma debe asegurar el cumplimiento con la Directiva de Máquinas (aunque sea para el propio uso de la compañía).

La Regulación 5 “Idoneidad del equipo de trabajo” es la parte central de la directiva y resalta la responsabilidad del empleador de llevar a cabo un proceso adecuado de evaluación de riesgos.

La Regulación 6 “Mantenimiento” requiere que la maquinaria reciba el servicio de mantenimiento apropiado. Esto normalmente significa que debe haber un programa rutinario y planificado de mantenimiento preventivo. Se recomienda usar un registro y mantenerlo actualizado. Esto es especialmente importante en casos en los que el mantenimiento e inspección del equipo contribuyen a la seguridad e integridad continua de un dispositivo o sistema protector.

Regulaciones 11 a 24

Estas regulaciones abarcan peligros específicos y configuraciones de protección en las máquinas.

No se implementaron totalmente hasta el 1 de enero de 1997 para máquinas no modificadas existentes, en uso antes del 1 de enero de 1993. Se aplicaron inmediatamente para otros

equipos. Sin embargo, si el equipo cumple con las directivas pertinentes, por ej., la Directiva de maquinarias, cumplirá automáticamente con los requisitos correspondientes de las regulaciones 11 a 24, ya que éstas son de naturaleza similar a los EHSR de dicha directiva.

De particular interés es la Regulación 11, la cual proporciona una jerarquía de las medidas de protección. Éstas son:

1. Guardas de aislamiento fijas.
2. Otras guardas o dispositivos de protección.
3. Aparatos de protección (guías, fijadores, varillas de empuje, etc.).
4. La provisión de información, instrucciones, supervisión y formación técnica.

Estas medidas deben aplicarse desde la primera hasta donde sea práctico, y generalmente se requerirá una combinación de dos o más medidas.

Regulaciones de los EE.UU.

Esta sección presenta algunas de las regulaciones sobre seguridad de protecciones para máquinas industriales en los EE.UU. Éste es sólo un punto de inicio; los lectores deberán investigar más a fondo los requisitos de sus aplicaciones específicas y tomar medidas para asegurar que sus diseños, usos y procedimientos de mantenimiento y prácticas cumplan con sus propias necesidades así como con los códigos y regulaciones locales y nacionales.

Hay muchas organizaciones que promueven la seguridad industrial en los Estados Unidos. Estas incluyen:

1. Corporaciones, las cuales usan requisitos establecidos y establecen sus propios requisitos internos;
2. La OSHA (Occupational Safety and Health Administration);
3. Organizaciones industriales tales como National Fire Protection Association (NFPA), Robotics Industries Association (RIA) y Association of Manufacturing Technology (AMT); y los proveedores de productos y soluciones de seguridad, como Rockwell Automation.

Occupational Safety and Health Administration (OSHA)

En los Estados Unidos, uno de los principales impulsores de la seguridad industrial es la OSHA (Occupational Safety and Health Administration). La OSHA fue establecida en 1970 por una Ley del Congreso de los EE.UU. El propósito de esta ley es proporcionar condiciones de trabajo saludables y de seguridad y preservar los recursos humanos. La ley autoriza que el Secretario de Trabajo establezca estándares de seguridad y salud ocupacional obligatorios aplicables a los negocios que afectan el comercio interestatal. Esta Ley se aplicará con respecto al empleo realizado en un lugar de trabajo en un estado, el Distrito de Columbia, el Estado Asociado de Puerto Rico, las Islas Vírgenes, Samoa Americana, Guam, El territorio de las Islas del Pacífico, la Isla Wake, la Plataforma Continental Exterior, la Isla Johnson y la Zona del Canal.

El Artículo 5 de la Ley establece los requisitos básicos. Cada empleador proporcionará a cada uno de sus empleados empleo y un lugar de empleo libre de peligros reconocidos que causen o probablemente causen la muerte o lesiones físicas graves a sus empleados; y cumplirá con los estándares de seguridad y salud ocupacional promulgados bajo esta Ley.

El Artículo 5 también establece que cada empleado deberá cumplir con los estándares de seguridad y salud ocupacionales y todas las reglas, regulaciones y órdenes emitidas de conformidad con esta Ley, las cuales sean aplicables a sus propias acciones y conducta.

La ley de OSHA establece que la responsabilidad corresponde tanto al empleador como al empleado. Esto es muy diferente de la Directiva para maquinarias que requiere que los proveedores pongan en el mercado máquinas libres de peligros. En los EE.UU., un proveedor puede vender una máquina sin ninguna protección. El usuario debe añadir la protección para que la máquina sea segura. Si bien ésta era una práctica común cuando se aprobó la Ley, la tendencia es que los proveedores proporcionen máquinas con protección incorporada, ya que diseñar la seguridad incorporada en la máquina es mucho más económico que añadir la protección después que la máquina ha sido diseñada y construida. La intención de los estándares ahora es tratar que el proveedor y el usuario se comuniquen mutuamente los requisitos de protección de modo que las máquinas fabricadas sean no sólo seguras sino más productivas.

El Secretario de Trabajo tiene la autoridad de promulgar como estándar de seguridad o salud ocupacional cualquier estándar de consenso y cualquier estándar federal, a menos que la promulgación de dicho estándar no resulte en una seguridad o salud mejorada para empleados designados de manera específica.

OSHA lleva a cabo esta tarea publicando reglamentos en el Título 29 del Código de Reglamentos Federales (29 CFR). Los estándares pertinentes a las máquinas industriales son publicados por OSHA en Parte 1910 de 29 CFR. Estos están disponibles libremente en el sitio web de OSHA en www.osha.gov. A diferencia de la mayoría de estándares que son voluntarios, los estándares de OSHA son leyes.

Algunas de las secciones importantes que pertenecen a la seguridad de la máquina son:

A – Generalidades
B – Adopción y extensión de estándares federales establecidos
C – Disposiciones de seguridad y salud generales
H – Materiales peligrosos
I – Equipo de protección personal
J – Controles ambientales generales – incluye bloqueo-marcado de seguridad
O – Barreras protectoras en la máquina y maquinaria
R – Sectores especiales
S – Especificaciones eléctricas

Algunos estándares de OSHA se refieren a estándares voluntarios. El efecto legal de incorporar por referencia es que el material se trata como si fuera publicado en su totalidad en el Registro Federal. Cuando un estándar de consenso nacional se incorpora como referencia en una de las subpartes, dicho estándar se considera ley. Por ejemplo, NFPA 70, un estándar voluntario conocido como el Código Eléctrico Nacional de los EE.UU. se referencia en la Subparte S. Esto hace que los requisitos del estándar NFPA 70 sean obligatorios.

29 CFR 1910.147, en la Subparte J, abarca el control de la energía peligrosa. Esto se conoce como el estándar de bloqueo-marcado de seguridad. El estándar voluntario equivalente es ANSI Z244.1. En resumen, este estándar requiere que la alimentación eléctrica de la máquina se bloquee durante las tareas de servicio o mantenimiento. El propósito es evitar una activación o puesta en marcha intempestiva de la máquina que podría resultar en lesiones a los empleados.

Los empleadores deben establecer un programa y utilizar procedimientos para bloquear o etiquetar de manera apropiada los dispositivos con el objeto de aislar la energía, y por otro lado inhabilitar las máquinas o el equipo para evitar una activación o puesta en marcha inesperada, o la liberación de energía almacenada a fin evitar lesiones a los empleados.

Este estándar no abarca cambios y ajustes menores de las herramientas y otras actividades de servicio menores que se realizan durante las operaciones normales de producción, si son tareas de rutina, repetitivas e integrales al uso del equipo de producción, siempre y cuando el trabajo se realice usando medidas alternativas que proporcionen una protección eficaz. Las medidas alternativas incluyen los dispositivos de protección como cortinas de luz, tapetes de seguridad, enclavamiento de compuertas y otros dispositivos similares conectados a un sistema de seguridad. El reto para el diseñador y para el usuario de la máquina es determinar cuáles son las tareas “menores” y “de rutina, repetitivas e integrales”.

La Subparte O abarca “Protección de la maquinaria y la máquina”. Esta subparte enuncia los requisitos generales para todas las máquinas así como requisitos para algunas máquinas específicas. Cuando se constituyó la OSHA en 1970, adoptó muchos estándares ANSI existentes. Por ejemplo, B11.1 para prensas mecánicas eléctricas se adoptó como estándar 1910.217.

1910.212 es el estándar general de OSHA para las máquinas. Establece que debe proporcionarse uno o más métodos de protección de máquina para proteger al operador y a otros empleados en el área de la máquina contra peligros tales como los creados por el punto de operación, puntos de atrapamiento, partes giratorias, rebabas que salen disparadas y chispas. Siempre que sea posible deben incorporarse guardas a la máquina, o deben fijarse de alguna otra manera si por alguna razón no es posible incorporarse a la máquina. La guarda no debe representar un peligro de accidente por sí sola.

El “punto de operación” es el área de la máquina donde se realiza el trabajo relacionado con el material procesado. Deberá protegerse el punto de operación de una máquina cuya operación expone a un empleado a sufrir lesiones. El dispositivo protector debe cumplir con los estándares vigentes o, en ausencia de estándares específicos aplicables, deberá estar diseñado y construido para evitar que el operador tenga ninguna parte de su cuerpo en la zona de peligro durante el ciclo de operación.

La Subparte S (1910.399) establece los requisitos eléctricos de OSHA. Una instalación o equipo será considerado aceptable por el Subsecretario de Trabajo y aprobado de acuerdo al significado de esta Subparte S si ha sido aceptado, certificado, listado, etiquetado o de algún otro modo ha sido determinada su seguridad por parte de un laboratorio de prueba reconocido a nivel nacional (NRTL).

¿Qué es un equipo? Un término general que incluye materiales, conexiones, dispositivos, artefactos, accesorios y similares, usados como parte de una instalación eléctrica o en conexión con ésta.

¿Qué significa “Listado”? Un equipo está “listado” si es de un tipo mencionado en una lista que (a) es publicada por un laboratorio reconocido a nivel nacional que realiza inspecciones periódicas de la producción de tal equipo y (b) establece que dicho equipo cumple con estándares reconocidos a nivel nacional o ha sido probado y se ha determinado su seguridad para uso de una manera específica.

A julio de 2006, las siguientes compañías son laboratorios de prueba reconocidos a nivel nacional:

- Applied Research Laboratories, Inc. (ARL)
- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- Electrical Reliability Services, Inc. (ERS)
- Entela, Inc. (ENT)
- FM Global Technologies LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

Algunos estados han adoptados sus propios estándares locales de OSHA. Veinticuatro estados, Puerto Rico y las Islas Vírgenes tienen planes estatales aprobados por OSHA y han adoptado sus propios estándares y políticas de cumplimiento de normas. En su mayor parte, estos estados adoptan estándares idénticos a los federales de OSHA. Sin embargo, algunos estados han adoptado estándares diferentes aplicables a este tema o pueden tener políticas de cumplimiento de normas diferentes.

Las empresas deben reportar el historial de incidentes a la OSHA. OSHA compila las tasas de incidentes, transmite la información a las oficinas locales, y utiliza esta información para priorizar las inspecciones. Los impulsores de inspección clave son:

- Peligro inminente
- Catástrofes y fatalidades
- Quejas de los empleados
- Sectores altamente peligrosos
- Inspecciones locales planificadas
- Inspecciones de seguimiento
- Programas nacionales y de enfoque local

Las violaciones de los estándares de la OSHA pueden resultar en multas. El detalle de las multas es:

- Graves: hasta $7000 por violación
- No graves: a discreción, pero no más de $7000
- Repetitivas: hasta $70,000 por violación
- A sabiendas: hasta $70,000 por violación
- Violaciones que resultan en la muerte: penas adicionales
- No corregir la violación: $7000/día

La tabla que figura a continuación muestra las 14 citaciones principales de la OSHA desde octubre de 204 hasta septiembre de 2005.

Estándar	**Descripción**
1910.147	El control de energía peligrosa (bloqueo-marcado de seguridad)
1910.1200	Comunicación peligrosa
1910.212	Requisitos generales para todas las máquinas
1910.134	Protección respiratoria
1910.305	Métodos de cableado, componentes y equipo para uso general
1910.178	Camiones industriales
1910.219	Transmisión de potencia mecánica
1910.303	Requisitos generales
1910.213	Maquinaria de carpintería
19102.215	Maquinaria de ruedas abrasivas
19102.132	Requisitos generales
1910.217	Prensas mecánicas
1910.095	Exposición ocupacional a ruido
1910.023	Protección contra aberturas y agujeros en el suelo y las paredes

Regulaciones canadienses

En Canadá, la seguridad industrial se rige a nivel de provincias. Cada provincia tiene sus propias normativas que se deben mantener y respetar. Por ejemplo, Ontario estableció la Ley de Salud y Seguridad Ocupacional que establece los derechos y deberes de todas las partes en el lugar de trabajo. Su principal propósito es proteger a los trabajadores contra peligros de salud y seguridad en el trabajo. La ley establece procedimientos para resolver los peligros en el lugar de trabajo y para hacer cumplir la ley cuando el cumplimiento no se realiza voluntariamente.

Dentro de la Ley está la regulación 851, sección 7 que define la revisión de las normas de salud y seguridad antes del arranque. Esta revisión es un requisito obligatorio en Ontario para cualquier maquinaria nueva, reconstruida o modificada, y un ingeniero profesional debe general el informe respectivo.

Normas

Esta sección proporciona una lista de algunos de los estándares internacionales y nacionales típicos pertinentes a la seguridad de la máquina. No tiene el objeto de ser una lista completa sino de proporcionar información sobre los asuntos de seguridad de maquinaria están sujetos a estandarización.

Este capítulo debe leerse junto con el Capítulo 1.

Muchos países del mundo están trabajando para lograr una armonización global de estándares. Esto se observa de manera especial en el área de seguridad de la máquina. Los estándares globales de seguridad de maquinaria se rigen por dos organizaciones: ISO e IEC. Los estándares regionales y de los países todavía y apoyan los requisitos locales, pero muchos países se están dirigiendo al uso de los estándares internacionales producidos por ISO e IEC.

Por ejemplo, los estándares EN (Norma Europea) se usan en todos los países de la EEA. Todos los nuevos estándares EN están en línea con los estándares ISO e IEC, y en la mayoría de casos tienen texto idéntico.

La IEC abarca asuntos electrotécnicos y la ISO trata otros asuntos. La mayoría de países industrializados son miembros de la IEC y ISO. Los estándares de seguridad de la maquinaria son escritos por grupos de trabajo formados por expertos de muchos de los países industrializados del mundo.

En la mayoría de países los estándares pueden considerarse como voluntarios, mientras que las regulaciones son legalmente obligatorias. Sin embargo, los estándares generalmente se usan como interpretación práctica de las regulaciones. Por lo tanto, el entorno de los estándares y de las regulaciones está estrechamente vinculado.

Por favor consulte el catálogo de seguridad disponible en: www.ab.com/safety for a comprehensive list of standards.

ISO (International Organization for Standardization)

ISO es una organización no gubernamental formada por las entidades de estándares nacionales de la mayoría de países del mundo (157 países al momento de la impresión de este documento). Una secretaría central situada en Ginebra, Suiza, coordina el sistema. ISO genera estándares para diseñar, fabricar y usar maquinaria de una manera más eficiente, segura y limpia. Estos estándares también facilitan y permiten que sea más justo el comercio entre países.

Los estándares de la ISO pueden identificarse por las letras ISO.

Los estándares para máquinas ISO están organizados de la misma manera que los estándares de EN, en tres niveles: Tipo A, B y C (consulte la sección posterior en los Estándares Europeos Armonizados EN).

Para obtener más información, visite el sitio web de ISO: www.iso.org.

IEC (International Electrotechnical Commission)

La IEC prepara y publica estándares internacionales para tecnologías eléctricas, electrónicas y otras afines. A través de sus miembros, la IEC promueve la cooperación internacional en todos los temas de la estandarización electrotécnica y asuntos relacionados, tales como la evaluación de la conformidad con los estándares electrotécnicos.

Para obtener más información, visite el sitio web de IEC: www.iec/ch

Estándares Europeos armonizados de EN

Estos estándares son comunes a todos los países de la EEA y son producidos por las organizaciones de estandarización europea CEN y CENELEC. Su uso es voluntario, pero el diseño y la fabricación de equipos conforme a sus especificaciones es la manera más directa de demostrar cumplimiento con los EHSR.

Estos están divididos en 3 tipos: Estándares A, B y C.

ESTÁNDARES Tipo A: Abarcan aspectos aplicables a todos los tipos de máquinas.

ESTÁNDARES Tipo B: Subdivididos en 2 grupos.
ESTÁNDARES Tipo B1: Abarcan aspectos específicos de seguridad y ergonomía de la maquinaria.
ESTÁNDARES Tipo B2: Abarcan componentes y dispositivos protectores.

ESTÁNDARES Tipo C: Abarcan tipos o grupos específicos de máquinas.

Es importante notar que cumplir con un Estándar C proporciona la suposición automática de conformidad con los EHSR. En ausencia de un Estándar C adecuado, pueden usarse los Estándares A y B como prueba parcial o total de conformidad con los EHSR, indicando el cumplimiento con las secciones pertinentes.

Puede usarse el sistema solar como modelo de la relación de la directiva de máquinas con los estándares europeos. Los planetas representan los estándares, los cuales giran alrededor del sol, el cual representa la directiva de maquinarias. Las órbitas interiores son los estándares "A" y "B". Las órbitas exteriores representan los estándares "C".

Se han concertado acuerdos para lograr la colaboración entre CEN/CENELEC y entidades tales como ISO e IEC. Eventualmente, esto deberá resultar en la implementación de estándares comunes en todo el mundo. En la mayoría de casos un estándar EN tiene una contraparte en IEC o ISO. En general los dos textos serán iguales y cualquier diferencia regional se expresará en referencia con el estándar.

El Capítulo 2 lista algunos de los estándares de EN/ISO/IEC y otros estándares nacionales y regionales pertinentes a la seguridad de la maquinaria. Cuando un estándar de EN se muestra entre corchetes, significa que es idéntico o muy parecido al estándar de ISO o IEC. Para obtener una lista completa de los estándares de seguridad de maquinaria de EN visite: http://europa.eu.int/comm/enterprise/mechan_equipment/machinery/index.htm.

Estándares de los EE.UU.

Estándares de OSHA

Siempre que sea posible, OSHA promulga estándares de consenso nacional o estándares federales establecidos como estándares de seguridad. Las disposiciones obligatorias (es decir la palabra implica obligatorio) de los estándares, incorporados por referencia, tienen el mismo vigor y efecto que los estándares listados en la Parte 1910. Por ejemplo, el estándar de consenso nacional NFPA 70 se lista como documento de referencia en el Apéndice A de la Subparte S-Eléctricos de la Parte 1910 de 29 CFR. NFPA 70 es un estándar voluntario desarrollado por la National Fire Protection Association (NFPA). NFPA 70 se conoce también como el Código Eléctrico Nacional (NEC). Por incorporación, todos los requisitos mandatorios del NEC son mandatorios de OSHA.

Estándares de ANSI

El American National Standards Institute (ANSI) sirve como administrador y coordinador del sistema de estandarización voluntaria del sector privado de los Estados Unidos. Es una organización de miembros privada y sin fines de lucro, que tiene el apoyo de un grupo diverso de organizaciones de los sectores privado y público.

ANSI no desarrolla estándares sino que facilita el desarrollo de éstos mediante el establecimiento de consenso entre los grupos calificados. ANSI también asegura que los grupos calificados sigan los principios de abertura y consenso, y los procedimientos debidos. A continuación se ofrece una lista parcial de estándares de seguridad que pueden obtenerse mediante ANSI.

Estos estándares están categorizados como estándares de aplicación o estándares de construcción. Los estándares de aplicación definen cómo aplicar un dispositivo de protección a la maquinaria. Algunos ejemplos incluyen ANSI B11.1, que proporciona información sobre el uso de guardas de máquina en prensas mecánicas y ANSI/RIA R15.06, que describe el uso de dispositivos de seguridad para guarda de robot.

National Fire Protection Association (NFPA)

La National Fire Protection Association (NFPA) se organizó en 1896. Su misión es reducir el efecto de los incendios en la calidad de vida promoviendo códigos y estándares con base científica, así como investigación y educación sobre incendios y aspectos relacionados a la seguridad. La NFPA auspicia muchos estándares para ayudar a llevar a cabo su misión. Dos estándares muy importantes relacionados con la seguridad industrial y la protección son el Código Eléctrico Nacional (NEC) y el Estándar Eléctrico para maquinaria industrial.

La National Fire Protection Association ha actuado como patrocinador de la NEC desde 1911. El documento del código original se desarrolló en 1897 como resultado de los esfuerzos unidos de diversos intereses aliados en temas seguridad, electricidad y arquitectura. Desde entonces la NEC se ha actualizado muchas veces y el contenido de su estándar se revisa cada tres años. El Artículo 670 del NEC abarca algunos detalles sobre maquinarias industriales y refiere al lector al Estándar Eléctrico para Maquinarias Industriales, NFPA 79.

NFPA 79 es aplicable a equipos eléctricos/electrónicos, aparatos o sistemas de máquinas industriales que funcionan a un voltaje nominal de 600 volts o menos. El propósito de NFPA 79 es proporcionar información detallada para la aplicación de equipos, aparatos o sistemas eléctricos/electrónicos suministrados como parte de máquinas industriales que promueven la seguridad personal y de la propiedad. NFPA 79, que fue adoptada oficialmente por ANSI en 1962, es muy similar en contenido al Estándar IEC 60204-1.

Las máquinas que no están incluidas en los estándares específicos de la OSHA, deben estar libres de fuentes de peligro reconocidas que puedan causar la muerte o lesiones personales graves. Estas máquinas deben diseñarse y mantenerse de manera que se satisfagan o se superen los requisitos de los estándares industriales aplicables. NFPA 79 es un estándar que se aplicaría a las máquinas que no están específicamente cubiertas por los estándares de OSHA.

Estándares canadienses

Los estándares CSA reflejan un consenso nacional de productores y usuarios, entre ellos fabricantes, consumidores, vendedores minoristas, sindicatos y organizaciones profesionales y entidades gubernamentales. Los estándares son ampliamente usados por la industria y el comercio y a menudo son adoptados en sus regulaciones por los gobiernos municipales, provinciales y federales, particularmente en los campos de salud, seguridad y construcción, así como el medio ambiente.

Las personas, compañías y asociaciones en todo Canadá demuestran su apoyo al desarrollo de estándares de la CSA ofreciendo de manera voluntaria su tiempo y conocimiento para el trabajo que realiza el Comité de la CSA y apoyando los objetivos de la Asociación. El total de miembros de la CSA está formada por más de 7000 voluntarios de comités y 2000 asociados.

El Standards Council of Canada es la entidad coordinadora del Sistema de Estándares Nacionales, una federación de organizaciones independientes y autónomas que trabajan para el desarrollo y mejora de la estandarización voluntaria a favor de los intereses nacionales.

Estándares australianos

La mayoría de estos estándares están en línea con los estándares de ISO/IEC/EN equivalentes.

Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Teléfono: +61 2 8206 6000
Correo electrónico: mail@standards.org.au
Sitio web: www.standards.org.au

Para comprar copias de los estándares:
SAI Global Limited
286 Sussex Street, Sydney, NSW 2001
Teléfono: +61 2 8206 6000
Fax: +61 2 8206 6001
Correo electrónico: mail@sai-global.com
Sitio web: www.saiglobal.com/shop

Por favor consulte el catálogo de seguridad disponible en: www.ab.com/safety for a comprehensive list of standards.

Estrategia de seguridad

Desde un punto de vista puramente funcional, es mejor que una máquina realice su tarea de procesar material de la manera más eficiente posible. Pero para que una máquina sea viable, también debe ser segura. De hecho, la seguridad debe ser una consideración principal.

Para desarrollar una estrategia de seguridad adecuada existen dos pasos que funcionan coordinadamente, como se muestra a continuación.

EVALUACIÓN DE RIESGOS basada en un entendimiento claro de los límites y funciones de la máquina y las tareas que puede requerirse realizar en la máquina durante el transcurso de su vida útil.

Luego se procede a la **REDUCCIÓN DEL RIESGO** si es necesario y se seleccionan medidas de seguridad en base a la información derivada de la etapa de evaluación de riesgos.

La manera en que esto se ha realizado es la base de la ESTRATEGIA DE SEGURIDAD de la máquina.

Necesitamos seguir una lista de verificación y asegurar que todos los aspectos estén considerados y que el principio que debe prevalecer no se pierda en los detalles. Todo el proceso debe documentarse. Esto no sólo asegurará un trabajo más minucioso sino que también permitirá que los resultados estén disponibles para que sean verificados por terceros.

Esta sección se aplica tanto a los fabricantes como a los usuarios de la máquina. El fabricante necesita asegurar que su máquina pueda usarse de manera segura. La evaluación de riesgos debe comenzar en la fase de diseño de la máquina y debe considerar todas las tareas previsibles que necesitarán realizarse en la máquina. Esta estrategia basada en tareas en las etapas tempranas de la evaluación de riesgos es muy importante. Por ejemplo, puede haber una necesidad frecuente de ajustar las piezas móviles de la máquina. En la fase de diseño deberá ser posible diseñar medidas que permitirán realizar este procedimiento de manera segura. Si estas se omiten en una etapa temprana puede ser difícil o imposible implementarlas en una etapa posterior. Como resultado los ajustes de las piezas móviles probablemente todavía necesitarán realizarse pero tendrían que realizarse de una manera arriesgada o ineficiente (o ambas). Una máquina cuyas tareas han sido consideradas en su totalidad durante la evaluación de riesgos será una máquina más segura y más eficiente.

El usuario necesita asegurar que las máquinas en su entorno de trabajo sean seguras. Incluso si una máquina ha sido declarada segura por el fabricante, el usuario de la máquina deberá realizar una evaluación de riesgos para determinar si el equipo es seguro en su propio entorno. A menudo las máquinas se usan en circunstancias no previstas por el fabricante. Por ejemplo, una máquina fresadora usada en el taller de un colegio necesitará consideraciones adicionales con respecto a una que se usa en una sala de herramientas industriales.

También debe recordarse que si una compañía usuaria adquiere dos o más máquinas independientes y las integra en un proceso, ellos serán los fabricantes de la máquina combinada resultante.

Por lo tanto, consideremos ahora los pasos esenciales para obtener una estrategia de seguridad apropiada. Lo siguiente puede aplicarse a una instalación de fábrica existente o a una sola máquina nueva.

Evaluación de riesgos

Es un error considerar la evaluación de riesgos como una carga. Es un proceso útil que proporciona información vital y permite que el usuario o el diseñador tomen decisiones lógicas acerca de las maneras de lograr la seguridad.

Hay varios estándares que abarcan este tema. ISO 14121: “Principios de la evaluación de riesgos” e ISO 12100: “Seguridad de la máquina – Principios básicos” contienen orientación que se aplica de una manera más global.

Cualquiera que sea la técnica usada para llevar a cabo una evaluación de riesgos, un equipo de personas provenientes de diversas áreas generalmente producirá un resultado con una cobertura más amplia y un mejor equilibro que una sola persona.

La evaluación de riesgos es un proceso reiterativo; se realizará en diferentes etapas del ciclo de vida de la máquina. La información disponible variará de acuerdo con la etapa del ciclo de vida. Por ejemplo, una evaluación de riesgos realizada por un constructor de máquinas tendrá acceso a cada detalle de los mecanismos de la máquina y los materiales de construcción, pero probablemente una suposición sólo aproximada del entorno de trabajo en que se usará la máquina. Una evaluación de riesgos realizada por un usuario de la máquina no necesariamente tendría acceso a los detalles técnicos minuciosos pero tendrá acceso a acceso a todos los detalles del entorno de trabajo de la máquina. Lo ideal es que el resultado de una acción repetitiva sirva de aporte al siguiente proceso.

Determinación de los límites de la máquina

Esto incluye recolectar y analizar información respecto a las partes, mecanismos y funciones de una máquina. También será necesario considerar todos los tipos de interacción humana con la máquina y el entorno en el cual funcionará la máquina. El objetivo es obtener un entendimiento claro de la máquina y sus usos.

En los casos en que máquinas separadas estén vinculadas ya sea mecánicamente o por sistemas de control, estas deben considerarse como una sola máquina, a menos que estén “zonificadas” por medidas de protección apropiadas.

Es importante considerar todas las limitaciones y etapas de la vida de una máquina, incluyendo instalación, puesta en marcha, mantenimiento, desmantelamiento, correcto uso y operación así como las consecuencias de un mal uso o mal funcionamiento razonablemente previsible.

Identificación de tareas y peligros

Todos los peligros de la máquina deben identificarse y listarse en términos de su naturaleza y ubicación. Los tipos de peligro incluyen trituración, corte, enredo, expulsión de piezas, vapores, radiación, substancias tóxicas, calor, ruido, etc.

Los resultados del análisis de tareas debe compararse con los resultados de la identificación de peligros. Esto mostrará donde existe la posibilidad de convergencia de un peligro y una persona, es decir, una situación peligrosa. Todas las situaciones riesgosas deberán listarse. Podría ser que el mismo peligro pueda producir diferentes tipos de situaciones peligrosas, según la naturaleza de la tarea o la persona. Por ejemplo, la presencia de un técnico de mantenimiento muy diestro y con alta formación técnica puede tener diferentes implicaciones que la presencia de un encargado de limpieza no calificado y sin conocimiento de la máquina. En esta situación, si cada caso es listado y tratado por separado puede ser posible justificar diferentes medidas de protección para el técnico de mantenimiento que para el encargado de la limpieza. Si los casos no se listan y tratan por separado, entonces deberá utilizarse el peor de los casos y el técnico de mantenimiento y el encargado de la limpieza quedarán cubiertos por la misma medida de protección.

Algunas veces será necesario llevar a cabo una evaluación de riesgos general sobre una máquina existente que ya tiene medidas protectoras (por ejemplo, una máquina con piezas móviles peligrosas protegida por una puerta con guarda de enclavamiento). Las piezas móviles constituyen un peligro potencial que puede convertirse en un peligro real en el caso de fallo del sistema de enclavamiento. A menos que el sistema de enclavamiento ya haya sido validado (por ejemplo por una evaluación de riesgos o diseño conforme con un estándar apropiado), su presencia no deberá considerarse.

Estimación de los riesgos

Éste es uno de los aspectos más fundamentales de la evaluación de riesgos. Existen muchas maneras de abordar este tema y las siguientes páginas ilustran los principios básicos.

Cualquier máquina que tenga un potencial de situaciones peligrosas presenta un riesgo de evento peligroso (es decir, daño). Cuanto mayor es el riesgo, más importante es hacer algo al respecto. En un peligro el riesgo podría ser tan pequeño que podríamos tolerarlo y aceptarlo, pero en otro peligro el riesgo podría ser tan alto que necesitaríamos tomar medidas extremas para brindar protección. Por lo tanto, para tomar una decisión respecto a “si hacer algo y qué hacer para evitar el riesgo”, necesitamos cuantificarlos.

El riesgo a menudo se considera únicamente en términos de la severidad de la lesión en caso de un accidente. Debe tenerse en consideración la gravedad de la lesión potencial Y la probabilidad de su ocurrencia para calcular la cantidad de riesgo presente.

Las sugerencias para calcular riesgos proporcionadas en las siguientes páginas no se ofrecen como método definitivo ya que las circunstancias individuales pueden indicar la necesidad de un método diferente. SE HAN DISEÑADO ÚNICAMENTE COMO PAUTAS GENERALES PARA FOMENTAR EL USO DE UNA ESTRUCTURA METÓDICA Y DOCUMENTADA.

El sistema de puntos usado no se ha evaluado para ningún tipo particular de aplicación, por lo tanto puede no ser adecuado para algunas aplicaciones. El documento ISO TR (Informe técnico) 14121-2 “Evaluación de riesgos – Orientación práctica y ejemplos de métodos” ahora está disponible y proporciona orientación práctica muy útil.

La siguiente información tiene el propósito de explicar e ilustrar la sección de estimación de riesgos del estándar existente ISO 14121 “Principios de la evaluación de riesgos.”

Los siguientes factores se tienen en consideración:

- LA GRAVEDAD DE UNA LESIÓN POTENCIAL.
- LA PROBABILIDAD DE SU OCURRENCIA.

La probabilidad de la ocurrencia incluye dos factores:

- FRECUENCIA DE EXPOSICIÓN.
- PROBABILIDAD DE LESIÓN.

Trataremos cada factor independientemente y asignaremos valores a cada uno de estos factores.

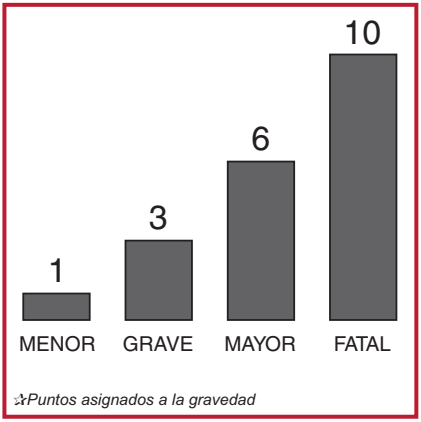
Use todos los datos y experiencia disponibles. Puesto que está tratando con todos las etapas de la vida útil de la máquina y para evitar una excesiva complejidad, base sus decisiones en el peor de los casos para cada factor.

También es importante usar el sentido común. Las decisiones deben tener en consideración lo que es factible, realista y posible. Es aquí donde es valioso un enfoque de un equipo que incluya miembros de diversas áreas.

Recuerde que para el propósito de este ejercicio, usted normalmente no debe tener en consideración ningún sistema protector existente. Si esta estimación de riesgos muestra que se requiere un sistema de protección, existen algunas metodologías mostradas posteriormente en este capítulo que pueden ser útiles para determinar las características requeridas.

1. La gravedad de una lesión potencial

Para esta consideración estamos asumiendo que ha ocurrido un accidente o incidente, quizás como resultado del peligro. Un estudio cuidadoso de la fuente de peligro revelará cuál es la lesión más grave posible. Recuerde: Para esta consideración estamos suponiendo que una lesión es inevitable y sólo estamos preocupados por su gravedad. Usted debe suponer que el operador está expuesto al movimiento o proceso peligroso. La gravedad de la lesión debe evaluarse como:



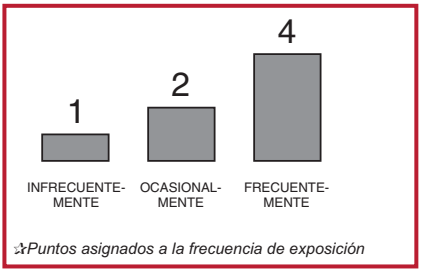
☆Puntos asignados a la gravedad

- FATAL: Muerte
- MAYOR: (Normalmente irreversible) Incapacidad permanente, pérdida de la vista, amputación de extremidad, daño respiratorio...
- GRAVE: (Normalmente reversible) Pérdida del conocimiento, quemaduras, roturas...
- MENOR: Magulladuras, cortes, abrasiones ligeras...

A cada descripción se le asigna el valor de puntos mostrado.

2. Frecuencia de exposición

La frecuencia de exposición responde a la pregunta de con qué frecuencia está expuesto al peligro el operador o la persona de mantenimiento. La frecuencia de la exposición al peligro puede clasificarse como:



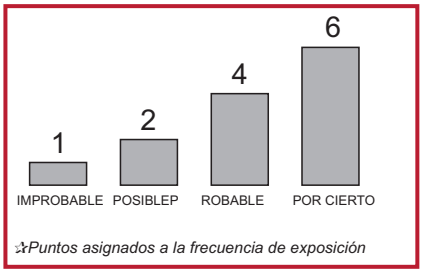
☆Puntos asignados a la frecuencia de exposición

- FRECUENTE: Varias veces al día.
- OCASIONAL: Diariamente.
- INFRECUENTE: Semanalmente o menos.

A cada descripción se le asigna el valor de puntos mostrado.

3 Probabilidad de lesión

Usted debe suponer que el operador está expuesto al movimiento o proceso peligroso. Al considerar la manera en la cual el operador está involucrado con la máquina y otros factores (velocidad de puesta en marcha, por ejemplo), la probabilidad de lesión puede clasificarse como:



☆Puntos asignados a la frecuencia de exposición

- IMPROBABLE
- POSIBLEP
- ROBABLE
- POR CIERTO

A cada descripción se le asigna el valor de puntos mostrado.

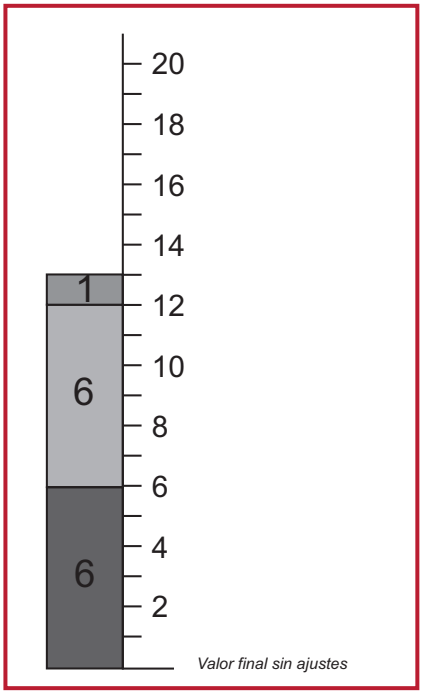
Se asigna un valor a todos los encabezados y ahora se suman para obtener un cálculo inicial. La suma de los tres componentes llega a un valor de 13. Pero debemos considerar algunos factores adicionales. (Nota: Esto no se basa necesariamente en las ilustraciones de los ejemplos previos).

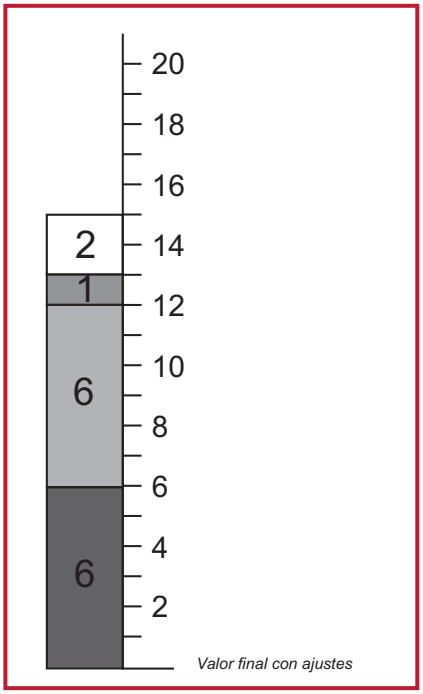
El siguiente paso es ajustar el cálculo inicial considerando factores adicionales tales como los indicados en la siguiente tabla. A menudo estos sólo pueden considerarse correctamente cuando la máquina está instalada en su ubicación permanente.

Factor típico	**Acción sugerida**
Más de una persona están expuestas al peligro	Multiplique el factor de gravedad por el número de personas
Tiempo prolongado en la zona de peligro sin un aislamiento completo de la alimentación eléctrica	Si el tiempo de cada acceso es más de 15 minutos, agregue 1 punto al factor de frecuencia
El operador es inexperto o no tiene la formación técnica requerida	Agregue 2 puntos al total
Intervalos muy largos (por ej., 1 año) entre accesos. (Pueden haber fallos progresivos y no detectados, especialmente en los sistemas de monitorización)	Añada puntos equivalentes al máximo factor de frecuencia

Consideraciones adicionales para la estimación de riesgos

Luego los resultados de los factores adicionales se suman al total previo, tal como se muestra.





Reducción del riesgo

Ahora debemos considerar cada máquina y sus riesgos respectivos y tomar medidas para solucionar todos sus peligros.

La siguiente tabla mostrada es una sugerencia para parte de un proceso documentado que considera todos los aspectos de seguridad de la maquinaria en uso. Debe usarse como guía para los usuarios de maquinaria, pero los fabricantes o proveedores de máquinas también pueden usar el mismo principio para confirmar que todo el equipo ha sido evaluado. También actuará como índice para informes más detallados sobre la evaluación de riesgos.

Esto muestra que cuando una máquina lleva la marca CE, simplifica el proceso porque los peligros de la máquina ya fueron evaluados por el fabricante y se han tomado todas las medidas necesarias. Aun con un equipo marcado con el distintivo CE, es posible que hayan peligros debido a la naturaleza de la aplicación o al material que se está procesando, lo cual no fue previsto por el fabricante.

Compañía – MAYKIT WRIGHT LTD
Instalación – Sala de herramientas – Fábrica del Este.
Fecha – 8/29/95
Perfil del operador – diestro.

Identificación y fecha del equipo	Cumplimiento con directiva	Número de Informe de evaluación de riesgos RA302	Historial de accidentes	Notas	Identificación del peligro	Tipo de peligro	Acción requerida	Implementado e inspeccionado – Referencia
Torno central Bloggs. Núm. de serie. 8390726 Instalado en 1978	Ninguno declarado		Ninguno	El equipo eléctrico cumple con la norma BS EN 60204 sobre paros de emergencia acoplados (reemplaz. en 1989)	Rotación del mandril con la guarda abierta	Corte por enredo mecánico	Acoplar interruptor de enclavamiento de guarda	11/25/94 J Kershaw, Informe Núm. 9567
					Fluido cortante	Tóxico	Cambiar a tipo no tóxico	11/30/94 J Kershaw, Informe Núm. 9714
					Limpiezas de rebabas	Corte	Suministrar guantes	11/30/94 J Kershaw, Informe Núm. 9715
Molino con cabeza de torre Bloggs m/c Núm. de serie. 17304294 Fabricado en 1995 Instalado en mayo 95	M/c Dir. EMC Dir	RA416	Ninguno		Movimiento de plataforma (hacia la pared)	Trituración	Mover máquina para dar espacio libre suficiente	4/13/95 J Kershaw, Informe Núm. 10064

Jerarquía de las medidas de reducción de riesgos

Existen tres métodos básicos que deben considerarse y usarse en el siguiente orden:

1. Eliminar o reducir riesgos en la medida de lo posible (diseño y construcción de máquina inherentemente segura),

2. Instalar los sistemas y medidas de protección necesarios (por ejemplo, guardas de enclavamiento, barreras de seguridad, etc.) en relación con los riesgos que no pueden ser eliminados por diseño.

3. Informar a los usuarios respecto a riesgos residuales debidos a deficiencias de las medidas de protección adoptadas, indicar si se requiere una formación técnica particular y especificar la necesidad de proporcionar equipo de protección personal.

Cada medida de la jerarquía debe considerarse, empezando por la primera, y usarse siempre que sea posible. Esto generalmente resultará en el uso de una combinación de medidas.

Diseño inherentemente seguro

En la fase de diseño de la máquina será posible evitar muchos de los posibles peligros simplemente mediante una consideración cuidadosa de factores tales como materiales, requisitos de acceso, superficies calientes, métodos de transmisión, puntos de atrapamiento, niveles de voltaje, etc.

Por ejemplo, si no se requiere acceso a un área peligrosa, la solución es protegerla dentro del cuerpo de la máquina o por algún tipo de guarda de aislamiento fija.

Sistemas y medidas de protección

Si se requiere acceso, entonces las cosas se complican un poco. Será necesario asegurar que sólo pueda obtenerse acceso mientras la máquina está en una condición de seguridad. Se requerirán medidas de protección tales como puertas de guarda enclavadas y/o sistemas de disparo. La selección del dispositivo o sistema dependerá significativamente de las características de operación de la máquina. Esto es extremadamente importante ya que un sistema que menoscaba la eficiencia de la máquina tiene el riesgo de que sea retirado u anulado sin autorización.

La seguridad de la máquina en este caso dependerá del uso apropiado y de la correcta operación del sistema de protección aun en condiciones de fallo.

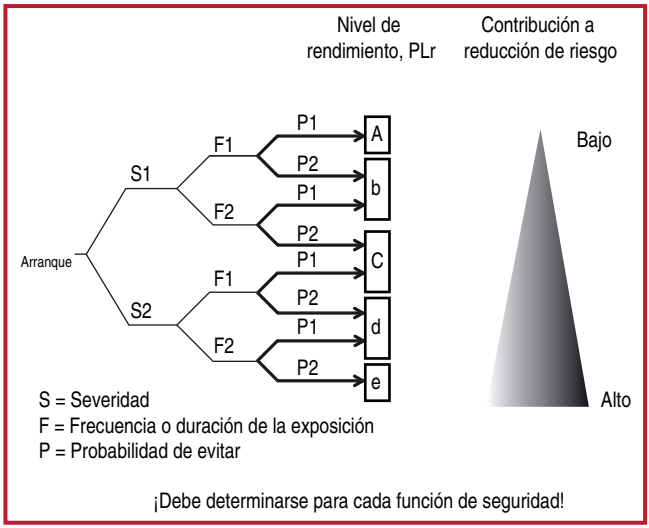
Ahora debe considerarse la correcta operación del sistema. Dentro de cada tipo es posible que haya una variedad de tecnologías con diversos grados de rendimiento de la monitorización, detección o prevención de fallos.

En condiciones ideales, cada sistema de protección sería perfecto sin posibilidades de fallo ni condiciones peligrosas. Sin embargo, en el mundo real, estamos restringidos por los límites actuales de conocimientos y materiales. Otra restricción muy real es el coste. Basado en estos factores, es obvio que se requiere un sentido de proporción. El sentido común nos indica que sería ridículo insistir en que la integridad de un sistema de seguridad de una máquina que puede causar, en el peor de los casos, magulladuras leves, sea igual a la integridad de un sistema requerido para mantener un avión en el aire. Las consecuencias de un fallo son drásticamente diferentes y por lo tanto necesitamos tener alguna manera de relacionar el grado de las medidas de protección con el nivel de riesgo obtenido en la etapa de estimación de los riesgos.

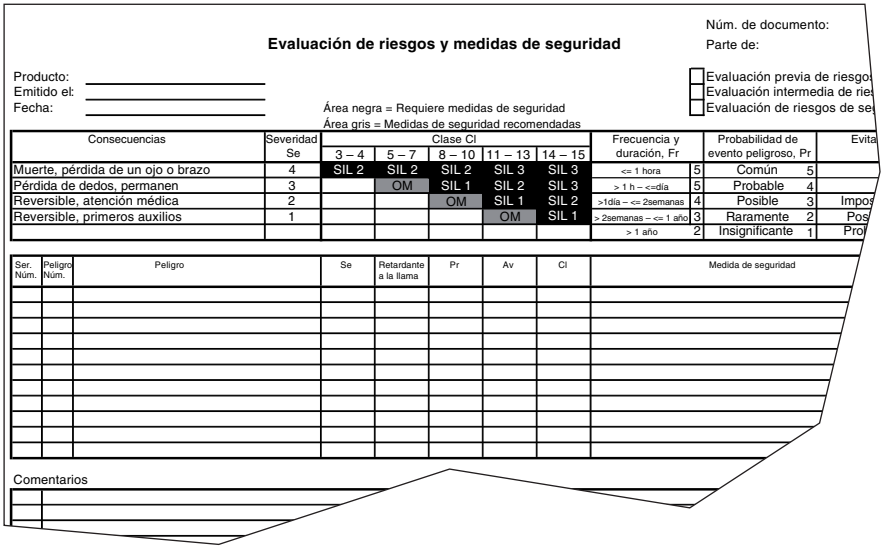
Independientemente del tipo de dispositivo protector seleccionado, debe recordarse que un “sistema relacionado a la seguridad” puede contener muchos elementos, entre ellos el dispositivo protector, el cableado, el dispositivo de conmutación de alimentación eléctrica y algunas veces partes del sistema de control operativo de la máquina. Todos estos elementos del sistema (incluyendo guardas, montaje, cableado, etc.) deben tener características de rendimiento apropiadas pertinentes a sus principios y tecnología de diseño. La versión pre-revisión del estándar ISO 13849-1 describe varias categorías para las partes de los sistemas de control relacionadas a la seguridad y proporciona un gráfico de riesgos en su Anexo B. Éste es un enfoque muy sencillo, pero puede proporcionar orientación útil para determinar algunos de los requisitos de un sistema de protección.

La versión revisada de los estándares ISO 13849-1 e IEC 62061 proporcionan métodos útiles y orientación sobre cómo especificar un sistema de control relacionado a la seguridad que proporcione una medida de protección o función de seguridad.

EN ISO 13849-1:2008 proporciona un gráfico de riesgos mejorado en su Anexo A.



IEC 62061 también proporciona un método en su Anexo A, el cual tiene el formato mostrado a continuación.



Evaluación de riesgos y medidas de seguridad

Núm. de documento:
Parte de:

Producto:
Emitido el:
Fecha:

☐ Evaluación previa de riesgos
☐ Evaluación intermedia de rie
☐ Evaluación de riesgos de se

Área negra = Requiere medidas de seguridad
Área gris = Medidas de seguridad recomendadas

Consecuencias	Severidad Se	Clase CI 3 – 4	5 – 7	8 – 10	11 – 13	14 – 15	Frecuencia y duración, Fr		Probabilidad de evento peligroso, Pr		Evita
Muerte, pérdida de un ojo o brazo	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 hora	5	Común	5	
Pérdida de dedos, permanen	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – <=día	5	Probable	4	
Reversible, atención médica	2			OM	SIL 1	SIL 2	>1día – <= 2semanas	4	Posible	3	Impos
Reversible, primeros auxilios	1				OM	SIL 1	> 2semanas – <= 1 año	3	Raramente	2	Pos
							> 1 año	2	Insignificante	1	Pro

Ser. Núm.	Peligro Núm.	Peligro	Se	Retardante a la llama	Pr	Av	Cl	Medida de seguridad

Comentarios

El uso de cualquiera de los métodos anteriores debe proporcionar resultados equivalentes. Cada método está diseñado para considerar el contenido detallado del estándar al cual pertenece.

En ambos casos es muy importante que se use la orientación provista en el texto del estándar. La Tabla o Gráfico de riesgos no debe usarse de una manera aislada o excesivamente simplista.

Evaluación

Después de seleccionar la medida de protección y antes de su implementación, es importante repetir la estimación del riesgo. Éste es un procedimiento que a menudo se omite. Puede darse el caso de que si instalamos una medida de protección, el operador de la máquina puede sentir que está total y completamente protegido contra el riesgo previsto. Puesto que ya no tiene la concienciación original del peligro, puede intervenir en la máquina de una manera diferente. Quizás estará expuesto al peligro con mayor frecuencia, acceda al interior de la máquina repetidamente. Esto significa que si la medida de protección falla, existirá un mayor riesgo que el previsto anteriormente. Éste es el riesgo real que debemos calcular. Por lo tanto, la estimación de riesgo debe repetirse teniendo en cuenta cualquier cambio previsto en la manera en que el personal puede intervenir en la máquina. El resultado de esta actividad se usa para verificar si las medidas de protección propuestas son, de hecho, apropiadas. Para obtener mayor información se recomienda que consulte el Anexo A de IEC 62061.

Formación técnica, equipo protector personal, etc.

Es importante que los operadores tengan la formación técnica necesaria en los métodos de trabajo seguro de una máquina. Esto no significa que pueden omitirse las otras medidas. No es aceptable simplemente indicar a un operador que no debe acercarse a las áreas peligrosas (como alternativa de protección).

También puede ser necesario que el operador use equipos como guantes especiales, gafas de protección, máscaras, etc. El diseñador de la maquinaria debe especificar el tipo de equipo requerido. El uso de equipo de protección personal generalmente no constituirá el método de protección principal sino que complementará las medidas indicadas anteriormente.

Estándares

Muchos estándares e informes técnicos proporcionan orientación para la evaluación de riesgos. Algunos se escriben para un uso amplio y otros para aplicaciones específicas.

La siguiente es una lista de estándares que incluye información sobre la evaluación de riesgos.

ANSI B11.TR3: Evaluación de riesgos y reducción de riesgos – Una guía para calcular, evaluar y reducir riesgos asociados con máquinas herramienta.

ANSI PMMI B155.1: Requisitos de seguridad para maquinaria de envasado y maquinaria de conversión relacionada al envasado

ANSI RIA R15.06: Requisitos de seguridad para robots y sistemas robóticos industriales

AS 4024.1301-2006: Principios de la evaluación de riesgos

CSA Z432-04: Protección de maquinaria

CSA Z434-03: Robots y sistemas robóticos industriales – Requisitos de seguridad generales

IEC/EN 61508: “Seguridad funcional de sistemas relacionados con la seguridad eléctricos, electrónicos y electrónicos programables”.

IEC/EN 62061: Seguridad funcional de sistemas de control eléctricos, electrónicos y programables relacionados con la seguridad.

ISO 14121 (EN 1050): Principios de la evaluación de riesgos.

Medidas de protección y equipo complementario

Cuando la evaluación de riesgos muestra que una máquina o proceso tiene el riesgo de causar lesiones personales, la fuente de peligro debe eliminarse o minimizarse. La manera de hacer esto dependerá del tipo de máquina y la fuente de peligro. Las medidas de protección se definen como métodos que evitan el acceso a un peligro o detectan el acceso a un peligro. Las medidas de protección incluyen dispositivos tales como guardas fijas, guardas de enclavamiento, barreras de seguridad, tapetes de seguridad, controles de bimanuales e interruptores de habilitación.

Cómo evitar el acceso con guardas de aislamiento fijas

Si la fuente de peligro se encuentra en una parte de la máquina que no requiere acceso, debe tener una guarda fija permanentemente en la maquinaria. Estos tipos de guardas deben requerir herramientas para su desinstalación. Las guardas fijas deben 1) resistir su entorno de operación, 2) contener proyectiles si es necesario y 3) no crear peligros mediante bordes puntiagudos, por ejemplo. Las guardas fijas pueden encajes donde la guarda se acople con la maquinaria o un envolvente de tipo malla de alambre.

Las ventanas proporciona maneras convenientes de monitorizar el rendimiento de la máquina, cuando se accede a una sección de la misma. Se debe tener en cuenta el material usado en esas ventas, ya que las interacciones de los productos químicos con los fluidos cortantes, rayos ultravioleta o el simple envejecimiento causan que los materiales de las mismas se degraden con el transcurso del tiempo.

El tamaño de las aberturas debe impedir que el operador llegue al peligro. La tabla O-10 de U.S. OHSA 1910.217 (f) (4), ISO 13854, Tabla D-1 de ANSI B11.19, Tabla 3 de CSA Z432 y AS4024.1 proporcionan orientación sobre la distancia apropiada a las piezas de riesgo a la que debe estar una abertura específica.

Detección de acceso

Se usan medidas de protección para detectar el acceso a un peligro. Cuando se selecciona la detección como método de reducción de riesgos, el diseñador debe entender que debe usarse un sistema de seguridad completo; el dispositivo de protección, por sí mismo, no proporciona la reducción de riesgo necesaria.

Este sistema de seguridad generalmente consta de tres bloques: 1) un dispositivo de entrada que detecta el acceso al peligro, 2) un dispositivo lógico que procesa las señales del dispositivo detector, verifica el estado del sistema de seguridad y activa o desactiva los dispositivos de salida y 3) un dispositivo de salida que controla el accionamiento (por ejemplo, un motor).

Dispositivos de detección

Muchos dispositivos alternativos están disponibles para detectar la presencia de una persona que accede o que está dentro del área peligrosa. La mejor opción para una aplicación particular depende de una serie de factores.

- La frecuencia del acceso,
- El tiempo de paro de la pieza de peligro,
- La importancia de completar el ciclo de la máquina, y
- La contención de proyectiles, fluidos, nubes tóxicas, vapores, etc.

Las guardas móviles seleccionadas de manera adecuada pueden enclavarse para proporcionar protección contra proyectiles, fluidos, nubes tóxicas y otros tipos de peligros, y a menudo se usan cuando el acceso al peligro es poco frecuente. Las guardas de enclavamiento también pueden bloquearse para evitar el acceso mientras la máquina está en el medio del ciclo y cuando la máquina requiere un tiempo prolongado para detenerse.

Los dispositivos de detección de presencia, como barrera de seguridad, alfombras sensibles y escáneres, proporcionan un acceso rápido y fácil al área de la pieza de peligro y generalmente se seleccionan cuando los operadores deben tener acceso frecuente al área del peligro. Estos tipos de dispositivos no proporcionan protección contra proyectiles, nubes tóxicas. fluidos u otros tipos de peligros.

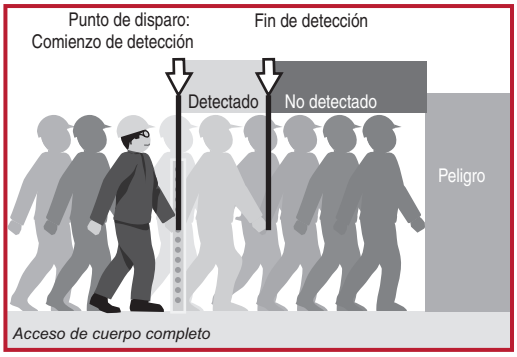
La mejor selección de una medida de protección es un dispositivo o sistema que proporcione la máxima protección con la mínima obstrucción de la operación normal de la máquina. Todos los aspectos del uso de la máquina deben considerarse, ya que la experiencia demuestra que es más probable que un sistema difícil de usar sea retirado o pasado por alto.

Dispositivos para detección de presencia

Cuando se decide cómo proteger una zona o área, es importante tener un claro entendimiento de qué funciones de seguridad se requieren exactamente. En general habrán por lo menos dos funciones.

- Desactivar o desconectar la alimentación eléctrica cuando una persona entra al área de peligro.
- Evitar activar o conectar la alimentación eléctrica cuando una persona está en el área de peligro.

En un inicio podría parecer que estas dos funciones son la misma cosa, pero aunque obviamente están vinculadas y generalmente son realizadas por el mismo equipo, en realidad son dos funciones diferentes. Para lograr el primer punto, necesitamos usar alguna forma de dispositivo de disparo. En otras palabras, un dispositivo que detecte que una parte de una persona ha pasado más allá de un punto específico y proporcione una señal para desconectar la alimentación eléctrica. Si la persona puede continuar pasado este punto de disparo y su presencia ya no es detectada, entonces puede que no se logre el segundo punto (evitar la activación).



El siguiente diagrama muestra un ejemplo de acceso del cuerpo completo con una barrera de seguridad montada verticalmente como dispositivo de disparo. Las puertas de guarda enclavadas también pueden considerarse como dispositivo de disparo solamente cuando no hay nada que pueda evitar que la puerta se cierre después de la entrada.

Si el acceso de todo el cuerpo no es posible y por lo tanto una persona no puede continuar más allá del punto de disparo, su presencia siempre es detectada y se logra el segundo punto (evitar la activación).

Para aplicaciones con acceso parcial del cuerpo, los mismos tipos de dispositivos realizan detección de presencia y disparo. La única diferencia es el tipo de aplicación.

Los dispositivos de detección de presencia se usan para detectar la presencia de las personas. La familia de dispositivos incluye barreras de seguridad, barreras de seguridad de un solo haz, escáneres de área de seguridad, alfombras sensibles de seguridad y bordes de seguridad.

Barreras de seguridad

Las barreras de seguridad son detectores de presencia fotoeléctricos diseñados específicamente para proteger al personal de lesiones relacionadas a movimiento peligroso de la máquina. Conocidas también como AOPD (dispositivos de protección optoelectrónica activa) o ESPE (equipo protector electrosensible) las barreras ofrecen una seguridad óptima, permiten mayor productividad y son la solución más ergonómica en comparación con las guardas mecánicas. Son ideales para aplicaciones en las que el personal necesita acceder fácilmente y con frecuencia a un punto de operación que presenta algún tipo de peligro.

Las barreras de seguridad están diseñadas y probadas para cumplir con los estándares IEC 61496-1 y -2. El Anexo IV de la Directiva europea para maquinarias requiere certificación de terceros para las barreras de seguridad antes de colocarlas en el mercado de la Unidad Europea. Terceros prueban las barreras de seguridad para asegurar que cumplen con este estándar internacional. Underwriter's Laboratory ha adoptado IEC 61496-1 como estándar nacional de los EE.UU.

Escáneres de láser de seguridad

Los escáneres láser de seguridad usan un espejo giratorio que desvía los pulsos de luz sobre un arco, creando un plano de detección. La ubicación del objeto es determinada por el ángulo de rotación del espejo. Mediante una técnica de “tiempo de vuelo” de un haz reflejado de luz invisible, el escáner también puede detectar la distancia a la que está el objeto del escáner. Al tomar la distancia medida y la ubicación del objeto, el escáner de láser determina la posición exacta del objeto.

Alfombras de seguridad para el suelo sensibles a la presión

Estos dispositivos se usan para proporcionar resguardo de una área del suelo alrededor de una máquina. Se coloca una matriz de tapetes interconectados alrededor del área de peligro y la presión aplicada a la alfombra (por ej., la pisada de un operador) causará que la unidad controladora de la alfombra desactive la alimentación eléctrica a la pieza peligrosa. Las alfombras sensibles a la presión generalmente se usan dentro de un área cerrada que contiene varias máquinas – celdas robóticas o de manufactura flexible, por ejemplo. Cuando se requiere acceso a la celda (para el establecimiento o “aprendizaje” del robot, por ejemplo), éstos evitan un movimiento peligroso si el operador se sale del área de seguridad o si debe ponerse detrás de una zona de riesgo.

El tamaño y posicionamento de la alfombra deben considerar la distancia de seguridad.

Bordes sensibles a la presión

Estos dispositivos son tiras que pueden montarse al borde de una pieza móvil, tal como la mesa o la puerta eléctrica de una máquina, la cual constituye un riesgo de trituración o corte.

Si la pieza móvil golpea al operador (o viceversa), el borde sensible flexible se oprime e iniciará un comando para desactivar la fuente de energía de la pieza peligrosa. Los bordes sensibles también pueden usarse para resguardar maquinaria cuando existe el riesgo de atrapamiento. Si la máquina atrapa a un operador, el contacto con el borde sensible desactivará la alimentación eléctrica de la máquina.

Hay una serie de tecnologías usadas para crear los bordes de seguridad. Una tecnología popular es insertar lo que esencialmente es un interruptor largo dentro del borde. Este método proporciona bordes rectos y generalmente utiliza la tecnología de conexión de 4 cables.

Las barreras de seguridad, los escáneres, las alfombras sensibles para el suelo y los bordes sensibles se clasifican como “dispositivos de disparo”. No restringen el acceso, lo “detectan”. Se basan totalmente en su capacidad de detección y conmutación para la provisión de seguridad. Generalmente son adecuados sólo para maquinarias que se detienen razonablemente rápido después que se desconecta la alimentación eléctrica. Puesto que un operador puede caminar o entrar directamente al área peligrosa, obviamente es necesario que el tiempo requerido para que el movimiento se detenga sea menor que el tiempo requerido para que el operador entre en contacto con la zona peligrosa.

Consulte www.ab.com/safety para obtener más información sobre la detección de presencia.

Interruptores de seguridad

Cuando el acceso a la máquina no es frecuente, es preferible usar guardas móviles (operables). La guarda se enclava con el suministro de energía de la pieza de peligro de manera que asegure que cada vez que la puerta de la guarda no esté cerrada, se desactivará la alimentación eléctrica de la zona de peligro. Este método requiere el uso de un interruptor de enclavamiento acoplado a la puerta de la guarda. El control de la fuente de energía de la zona de peligro es controlado a través de la sección de conmutación de la unidad. La fuente de energía es generalmente eléctrica, pero podría ser también neumática o hidráulica. Cuando se detecta movimiento (abertura) de la puerta de la guarda, el interruptor de enclavamiento iniciará un comando para aislar el suministro de energía de ya sea directamente, mediante un contactor de alimentación eléctrica o válvula.

Algunos interruptores de enclavamiento también incorporan un dispositivo de enclavamiento que enclava la puerta de la guarda en posición cerrada y no permite que se abra hasta que la máquina esté en una condición segura. En la mayoría de aplicaciones, la combinación de una guarda movible y un interruptor de enclavamiento con o sin bloqueo de la guarda es la solución más fiable y económica.

Existe una amplia variedad de opciones de interruptores de seguridad, entre ellos:

- **Interruptores con enclavamiento de lengüeta** – estos dispositivos requieren la inserción y retiro de un accionador en forma de lengüeta del interruptor para su operación
- **Interruptores de enclavamiento de bisagra** – estos dispositivos se colocan sobre el pin de bisagra de una puerta de guarda y utilizan la acción de abertura de la guarda para el accionamiento.
- **Interruptores de bloqueo de guarda** – En algunas aplicaciones, se requiere el bloqueo de la guarda cerrada o retardar la abertura de la guarda. Los dispositivos adecuados para este requisitos se llaman interruptores de enclavamiento con bloqueo de guarda. Estos dispositivos son apropiados para máquinas con retardo al paro, pero también pueden ofrecer un aumento significativo del nivel de protección para la mayoría de tipos de máquinas.
- **Interruptores de enclavamiento sin contacto** – estos dispositivos no requieren contacto físico para actuar con algunas versiones que incorporan una función de codificación para mayor resistencia a las intrusiones.
- **Dispositivos de enclavamiento de posición (interruptor de final de carrera)** – El accionamiento operado por levas generalmente toma la forma de un interruptor de final de carrera (o posición) positivo y una leva lineal o giratoria. Generalmente se usa en guardas deslizantes.

- **Dispositivos de enclavamiento con atrapamiento de guarda** – Las llaves bloqueo mecánico secuencial pueden realizar enclavamiento de control así como enclavamiento de la alimentación eléctrica. Con el “enclavamiento de control” un dispositivo de enclavamiento inicia un comando de paro a un dispositivo intermedio, el cual desactiva un dispositivo subsiguiente para desconectar la energía del accionador. Con el “enclavamiento de la alimentación eléctrica”, el comando de paro interrumpe directamente el suministro de energía a los accionadores de la máquina.

Interfaces operador-máquina

Función de paro – en los EE.UU., Canadá, Europa y a nivel internacional, existe armonización de estándares con respecto a las descripciones de las categorías de paro para máquinas o sistemas de fabricación.

NOTA: estas categorías son diferentes a las categorías de EN 954-1 (ISO 13849-1). Vea Estándares NFPA 79 e IEC/EN 60204-1 para obtener más detalles. Las funciones de parada pertenecen a tres categorías:

Categoría 0 es paro mediante desconexión inmediata de la alimentación eléctrica a los accionadores de la máquina. Esto se considera paro no controlado. Con la alimentación eléctrica desconectada, la acción de freno que requiere alimentación eléctrica no será eficaz. Esto permitirá que los motores giren libremente y paren por inercia en un período de tiempo extendido. En otros casos, la máquina que está reteniendo accesorios puede dejar caer material, lo cual requiere alimentación eléctrica para retener el material. También puede usarse medios de paro mecánico que no requieren alimentación eléctrica con un paro de categoría 0. El paro de categoría 0 tiene prioridad sobre los paros de categoría 1 ó 2.

Categoría 1 es un paro controlado con alimentación eléctrica disponible a los accionamientos de la máquina para realizar el paro. Luego, cuando se realiza el paro, la alimentación eléctrica se desconecta de los accionamientos. Esta categoría de paro permite que el freno energizado detenga rápidamente el movimiento peligroso y luego la alimentación eléctrica puede desconectarse de los accionamientos.

Categoría 2 es un paro controlado con alimentación eléctrica disponible a los de la máquina. Un paro de producción normal se considera paro de categoría 2.

Estas categorías de paro deben aplicarse a cada función de parada, cuando es la acción tomada por los dispositivos de control de seguridad en respuesta a una señal de entrada, la categoría 0 ó 1 debería utilizarse. Las funciones de paro deben anular las funciones de arranque relacionadas. La selección de la categoría de paro de cada función de paro debe determinarse mediante una evaluación de riesgos.

Función de paro de emergencia

La función de paro de emergencia debe funcionar como paro de categoría 0 o categoría 1, según lo determinado por una evaluación de riesgos. Debe ser iniciada por una sola acción humana. Cuando se ejecuta, debe anular todas las otras funciones y modos de operación de la máquina. El objetivo es desconectar la alimentación eléctrica tan rápidamente como sea posible sin crear peligros adicionales.

Hasta hace poco, se requerían componentes electromecánicos cableados para circuitos de paro de emergencia. Los cambios recientes en estándares tales como IEC 60204-1 y NFPA 79 significan que los PLC de seguridad y otras formas de lógica electrónica que cumplen con los requisitos de estándares como IEC 61508, pueden usarse en el circuito de paro de emergencia.

Dispositivos de paro de emergencia

Siempre que exista el peligro de que un operador corra algún riesgo con una máquina, deben instalarse facilidades para un acceso rápido a un dispositivo de paro de emergencia. El dispositivo de paro de emergencia debe estar operativo continuamente y fácilmente accesible. Los paneles de operador deben tener por lo menos un dispositivo de paro de emergencia. Otros dispositivos de emergencia pueden utilizarse en otros lugares, según sea necesario. Los dispositivos de paro de emergencia vienen en diversos formatos. Algunos ejemplos populares son los interruptores de botón pulsador y los interruptores accionados por cable. Cuando se acciona el dispositivo de paro de emergencia, éste debe enclavarse y no debe ser posible generar el comando de paro sin enclavarlo. El restablecimiento del dispositivo de paro de emergencia no debe causar una situación peligrosa. Una acción separada y deliberada debe utilizarse para volver a arrancar la máquina.

Para obtener más información sobre dispositivos de paro de emergencia, lea ISO/EN 13850, IEC 60947-5-5, NFPA 79 e IEC 60204-1, AS4024.1, Z432-94.

Botones de paro de emergencia

Los dispositivos de paro de emergencia se consideran equipo de protección complementaria. No se consideran dispositivos de protección primaria porque no evitan el acceso a una pieza peligrosa o no detectan el acceso a una pieza peligrosa.

La manera usual de proporcionar esto es mediante un botón pulsador de seta de color rojo sobre fondo amarillo que el operador presiona en caso de una emergencia (vea la Figura 4.59). Deben estar colocados estratégicamente en suficiente cantidad alrededor de la máquina para asegurar que siempre haya uno al alcance en un punto peligroso.

Los botones de paro de emergencia deben estar accesibles y disponibles en todos los modos de operación de la máquina. Cuando se use un botón pulsador como dispositivo de paro de emergencia, éste debe ser del tipo hongo (o de operación con la palma de la mano) y debe ser de color rojo con fondo amarillo. Cuando se oprima el botón, los contactos deben cambiar de estado a la vez que el botón se enclava en la posición de oprimido.

Una de las más recientes tecnologías que se aplican a los paros de emergencia es la técnica de automonitorización. Se añade un contacto adicional en la parte posterior del paro de emergencia que monitoriza si la parte trasera de los componentes del panel todavía están presentes. Esto se conoce como bloque de contactos automonitorizados. Consta de un contacto accionado por resorte que se cierra cuando el bloque de contactos se encaja en su lugar en el panel. La Figura 4.60 muestra el contacto de automonitorización conectado en serie con uno de los contactos de seguridad de apertura directa.

Interruptores accionados por cable

Para maquinarias tales como transportadores, generalmente es más conveniente y eficaz usar un dispositivo accionado por cable a lo largo del área peligrosa (tal como se muestra en la Figura 4.61.) como dispositivo de paro de emergencia. Estos dispositivos usan un cuerda de acero conectada a los interruptores de accionamiento por cuerda de manera que al tirar de la cuerda en cualquier dirección y en cualquier punto a lo largo de su longitud se accionará el interruptor y se cortará la alimentación eléctrica de la máquina.

Los interruptores accionados por cable deben detectar que es accionado así como cuando el cable tiene holgura. La detección de holgura asegura que no se corte el cable y que está listo para ser usado.

El recorrido del cable afecta el rendimiento del interruptor. Para distancias cortas, el interruptor de seguridad se monta en un extremo y un resorte de tensión se monta en el otro. Para distancias mayores debe montarse un interruptor de seguridad en ambos extremos del cable para asegurar que una acción única por parte del operador inicie un comando de paro. La fuerza de accionamiento del interruptor del cable requerida no debe exceder de 200 N (45 lbs) ni una distancia de 400 mm (15.75 pulg.) en una posición centrada entre dos soportes de cable.

Controles bimanuales

El uso de los controles bimanuales (llamados también controles dobles) es un método común de evitar el acceso mientras la máquina está en una condición peligrosa. Dos controles deben operarse concurrentemente (a 0.5 s uno de otro) para arrancar la máquina. Esto asegura que ambas manos del operador estén ocupadas en una posición segura (por ej., en los controles) y por lo tanto no puedan estar en el área peligrosa. Los controles deben operarse continuamente durante las condiciones peligrosas. La operación de la máquina debe detenerse cuando se libera cualquiera de los controles. Si un control es liberado el otro control también debe liberarse para que pueda arrancar la máquina.

Un sistema de dos manos depende en gran medida de la integridad de su sistema de control y monitorización para detectar cualquier fallo, por lo tanto es importante que este aspecto esté diseñado según la especificación correcta. El rendimiento de un sistema de seguridad bimanuales está caracterizado en tipos por ISO 13851 (EN 574) como se muestra, y están relacionados a las Categorías de ISO 13849-1. Los tipos más comúnmente usados para seguridad de maquinaria son IIIB e IIIC. La siguiente tabla muestra la relación de los tipos con respecto a las categorías de rendimiento de seguridad.

Requisito	Tipos				
	I	II	III		
			A	B	C
Accionamiento asíncrono			X	X	X
Use de la Categoría 1 (de ISO 13849-1)	X		X		
Use de la Categoría 3 (de ISO 13849-1)		X		X	
Use de la Categoría 4 (de ISO 13849-1)					X

La separación en el diseño físico debe impedir una operación incorrecta (por ej., con la mano y el codo). Esto puede realizarse mediante distancia o protectores. La máquina no debe ir de un ciclo a otro sin soltar y presionar ambos botones. Esto evita la posibilidad de bloquear ambos botones, dejando la máquina en funcionamiento continuo. El soltar cualquiera de los botones debe causar que la máquina se detenga.

El uso del control bimanuales debe considerarse con cautela ya que generalmente permite la exposición a algún tipo de riesgo. El control de dos manos sólo protege a la persona que los utiliza. El operador protegido debe ser capaz de observar todos los accesos a la pieza peligrosa, ya que otro personal quizás no esté protegido.

ISO 13851 (EN 574) proporciona orientación adicional sobre el control bimanuales.

Dispositivos de habilitación

Los dispositivos de habilitación son controles que permiten que un operador ingrese en un área peligrosa con la pieza peligrosa en operación mientras el operador sujeta el dispositivo de habilitación en posición de accionamiento. Los dispositivos de habilitación utilizan tipos de interruptores de dos o tres posiciones. Los tipos de dos posiciones están desactivados cuando no se opera el accionador y están activados cuando se opera el accionador. Los interruptores de tres posiciones están desactivados cuando no están accionados (posición 1), activados cuando se mantienen en la posición central (posición 2) y desactivados cuando el accionador se opera pasando la posición central (posición 3). Además, al regresar de la posición 3 a la posición 1, el circuito de salida no debe cerrarse al pasar a través de la posición 2.

Los dispositivos de habilitación deben usarse junto con otra función relacionada con la seguridad. Un ejemplo típico es colocar el movimiento en un modo lento controlado. Una vez que está en el modo lento, un operador puede entrar al área peligrosa sujetando el dispositivo de habilitación.

Al usar un dispositivo de habilitación, una señal debe indicar que el dispositivo de habilitación está activo.

Dispositivos lógicos

Los dispositivos lógicos desempeñan un papel central en la pieza relacionada a la seguridad del sistema de control. Los dispositivos lógicos realizan la verificación y monitorización del sistema de seguridad y permiten que la máquina arranque o ejecutan comandos para parar la máquina.

Hay una gama de dispositivos lógicos disponibles para crear una arquitectura de seguridad que satisfaga los requisitos de complejidad y funcionalidad de la máquina. Los relés de seguridad cableados de monitorización son más económicos para máquinas de menor tamaño que requieren un dispositivo lógico dedicado para completar la función de seguridad. Se prefieren relés de seguridad para monitorización modulares y configurables cuando se requiere un número grande y diverso de dispositivos de protección y control de zona mínimo. Para una máquina mediana a grande y más compleja serán preferibles los sistemas programables con E/S distribuidas.

Relés de control de seguridad

Los módulos de relé de control de seguridad (MSR) desempeñan un papel clave en muchos sistemas de seguridad. Estos módulos generalmente comprenden dos o más relés con guía positiva con circuitos adicionales para asegurar el rendimiento de la función de seguridad.

Los relés con guía positiva son relés de “cubo de hielo” especiales. Los relés con guía positiva deben cumplir con los requisitos de rendimiento de EN 50025. Esencialmente, están diseñados para evitar que los contactos normalmente cerrados y normalmente abiertos se cierren simultáneamente. Los diseños más nuevos reemplazan las salidas electromecánicas con salidas de seguridad de estado sólido.

Los relés de control de seguridad realizan muchas verificaciones en el sistema de seguridad. En el momento del encendido realizan autoverificaciones de sus componentes internos. Cuando los dispositivos de entrada se activan, el MSR compara los resultados de las entradas redundantes. Si son aceptables, el MSR verifica los accionadores externos. Si están bien, el MSR espera una señal de restablecimiento para activar sus salidas.

La selección del relé de seguridad apropiado depende de una serie de factores: el tipo de dispositivo que monitoriza, el tipo de restablecimiento, el número y tipo de salidas.

Tipos de entradas

Los dispositivos de protección tienen diferentes métodos para indicar que algo sucedió:

Dispositivos de enclavamiento con contactos y paro de emergencia: Contactos mecánicos, un solo canal con un contacto normalmente cerrado o dos canales, ambos normalmente cerrados. El MSR debe ser capaz de aceptar uno o dos canales y proporcionar detección de fallo cruzado para la configuración de dos canales.

Dispositivos de enclavamiento sin contactos y paro de emergencia: Contactos mecánicos, dos canales, uno normalmente abierto y uno normalmente cerrado. El MSR debe ser capaz de procesar diversas entradas.

Dispositivos de conmutación de estado sólido de salida: Las PNP, escáneres láser, dispositivos de estado sólido sin contacto tienen dos salidas surtidoras y realizan detección de fallo cruzado. El MSR debe ignorar el método de detección de fallo cruzado de los dispositivos.

Alfombras para el suelo sensibles a la presión: Los tapetes crean un cortocircuito entre dos canales. El MSR debe resistir los cortocircuitos repetidos.

Bordes sensibles a la presión: Algunos bordes están diseñados como los alfombras de 4 cables. Algunos son dispositivos de dos cables que crean un cambio en la resistencia. El MSR debe ser capaz de detectar un cortocircuito o el cambio de resistencia.

Voltaje: Mide el EMF regenerada de un motor durante el paro del mismo. El MSR debe tolerar altos voltajes así como detectar bajos voltajes a medida que el motor desacelera.

Interrupción de movimiento: El MSR debe detectar flujos de impulsos provenientes de diversos sensores redundantes.

Control de dos manos: El MSR debe detectar entradas diversas normalmente abiertas y normalmente cerradas y proporcionar temporización de 0.5 s y lógica de secuenciamiento.

Los relés de seguridad de monitorización deben diseñarse específicamente para hacer interfaz con cada uno de estos tipos de dispositivos, ya que tienen características eléctricas diferentes. Algunos MSR pueden hacer conexión con varios tipos de entradas diferentes, pero una vez que el dispositivo se ha seleccionado, el MSR sólo puede hacer interfaz con dicho dispositivo. El diseñador debe seleccionar un MSR compatible con el dispositivo de entrada.

Impedancia de entrada

La impedancia de entrada de los relés de control de seguridad determina cuántos dispositivos de entrada pueden conectarse al relé y a qué distancia máxima pueden montarse. Por ejemplo, un relé de seguridad puede tener una impedancia de entrada permitida máxima de 500 ohms. Cuando la impedancia de entrada es mayor que 50 ohms, éste no activará sus salidas. El usuario debe tener cuidado para asegurarse de que la impedancia de entrada permanezca debajo de la especificación máxima. La longitud, tamaño y tipo de cable usado afecta la impedancia de entrada.

Número de dispositivos de entrada

El proceso de evaluación de riesgos debe usarse para ayudar a determinar cuántos dispositivos de entrada deben conectarse a una unidad de relé de control de seguridad MSR y con qué frecuencia deben verificarse los dispositivos de entrada. Para asegurar que los dispositivos de paro de emergencia y los dispositivos de enclavamiento de compuerta estén en estado

operativo, su funcionamiento debe verificarse a intervalos regulares, según lo determinado por la evaluación de riesgos. Por ejemplo, un MSR de entrada de dos canales conectado a una compuerta enclavada que debe abrirse en cada ciclo de la máquina (por ej., varias veces al día) quizás no necesite verificarse. Esto se debe a que la abertura de la guarda hace que el MSR se autoverifique, así como sus entradas y sus salidas (dependiendo de la configuración) para determinar si tiene fallos individuales. A mayor frecuencia de abertura de la guarda, mayor integridad del proceso de verificación.

Otro ejemplo pueden ser los dispositivos de paro de emergencia. Puesto que los dispositivos de paro de emergencia normalmente sólo se usan para emergencias, éstos generalmente se usan muy poco. Por lo tanto, un programa debe establecerse para ejecutar los paros de emergencia y confirmar su efectividad según un cronograma especificado. Ejecutar un sistema de seguridad de esta manera se llama realizar una prueba de calidad, y el tiempo entre pruebas de calidad se llama intervalo de prueba de calidad. Un tercer ejemplo pueden ser las puertas de acceso para realizar ajustes en la máquina, las cuales, al igual que los paros de emergencia, pueden usarse con poca frecuencia. Aquí nuevamente debería establecerse una verificación de operatividad manual programada en el tiempo.

La evaluación de riesgos ayudará a determinar si los dispositivos de entrada necesitan verificarse y con qué frecuencia. A mayor nivel de riesgo, mayor integridad requerida del proceso de verificación. Y mientras menos frecuente sea la verificación “automática”, más frecuente deberá ser la verificación “manual” impuesta.

Detección de fallo cruzado de entrada

En sistemas de canal doble, los fallos de cortocircuito de canal a canal de los dispositivos de entrada, también conocidos como fallos cruzados, deben ser detectados por el sistema de seguridad. Esto es realizado por un dispositivo detector o por el relé de control de seguridad.

Los relés de control de seguridad basados en microprocesador, como las barreras de seguridad, los escáneres de láser y los sensores sin contacto más sofisticados detectan estos cortocircuitos de diversas maneras. Una manera común de detectar fallos cruzados es usar test de pulsos. Las señales de salida tienen pulsos muy rápidos. El pulso del canal 1 es offset del pulso del canal 2. Si se produce un cortocircuito, los pulsos ocurren concurrentemente y son detectados por el dispositivo.

Los relés de control de seguridad electromecánicos emplean una técnica diferente: una entrada de activación y una entrada de desactivación. Un cortocircuito del canal 1 al canal 2 hará que el dispositivo de protección contra sobrecorriente se active y el sistema de seguridad se desactivará.

Salidas

Los MSR vienen con diversos números de salidas. Los tipos de salidas ayudan a determinar qué MSR debe usarse en aplicaciones específicas.

La mayoría de MSR tienen por lo menos 2 salidas de seguridad de operación inmediatas. Las salidas de seguridad MSR se caracterizan por estar normalmente abiertas. Tienen clasificación de seguridad debido a la redundancia y verificación interna. Un segundo tipo de salida son las salidas retardadas. Las salidas retardadas generalmente se usan en paros de Categoría 1, donde la máquina requiere tiempo para ejecutar la función de paro antes de permitir acceso al área peligrosa. Los MSR también tienen salidas auxiliares. Generalmente estas se consideran normalmente cerradas.

Especificaciones de salida

Las especificaciones de salida describen la capacidad del dispositivo de protección de conmutar las cargas. Normalmente, las especificaciones de los dispositivos industriales se describen como resistivas o electromagnéticas. Una carga resistiva puede ser un elemento calefactor. Las cargas electromagnéticas son típicamente relés, contactores o solenoides con una gran característica inductiva de la carga. El Anexo A del estándar IEC 60947-5-1 describe las capacidades nominales de las cargas. Esto también se muestra en la sección ‘principios’ del catálogo de seguridad.

Letra de designación: La designación es una letra seguida por un número, por ejemplo A300. La letra se refiere a la corriente térmica convencional incluida y si dicha corriente es directa o alterna. Por ejemplo A representa 10 amps. de corriente alterna. Los números se refieren al voltaje de aislamiento nominal. Por ejemplo, 300 representa 300 V.

Utilización: La utilización describe los tipos de cargas que el dispositivo es capaz de conmutar. Las utilizaciones relevantes a IEC 60947-5 se muestran en la siguiente tabla.

Utilización	Descripción de la carga
AC-12	Control de cargas resistivas de estado sólido con aislamiento por optoacopladores
AC-13	Control de cargas de estado sólido con aislamiento de transformador
AC-14	Control de cargas electromagnéticas (menores de 72 VA's)
AC-15	Cargas electromagnéticas mayores de 72 Va's
DC-12	Control de cargas resistivas de estado sólido con aislamiento por optoacopladores
DC-13	Control de cargas electromagnéticas
DC-14	Control de cargas electromagnéticas que tienen resistencias en el circuito

Corriente térmica, Ith: La corriente térmica incluida convencional es el valor de corriente usado para las pruebas de subida de temperatura del equipo cuando está montado en un envolvente especificado.

Voltaje Ue y corriente de operación nominal; El voltaje y la corriente de operación nominal especifican las capacidades de cierre y apertura de los elementos de conmutación bajo condiciones de operación normal. La capacidad nominal de los productos Guardmaster de Allen-Bradley es 125 VCA, 250 VCA y 24 VCC. Consulte con la fábrica para obtener información sobre uso a voltajes diferentes a estas capacidades nominales especificadas.

VA: Las especificaciones de VA (Voltaje x Amperios) indican las especificaciones de los elementos de conmutación cuando se cierra el circuito y cuando se abre el circuito.

Ejemplo 1: Una capacidad nominal de A150, CA-15 indica que los contactos pueden cerrar un circuito de 7200 VA. A 120 VCA, los contactos pueden cerrar un circuito de entrada al momento del arranque de 60 amp. Puesto que CA-15 es una carga electromagnética, los 60 amp tienen una corta duración al momento del arranque de la carga. La apertura del circuito es sólo 720 VA porque la corriente de mantenimiento de la carga es de 6 A, o sea la corriente nominal o de consumo.

Ejemplo 2: Una capacidad nominal de N150, DC-13 indica que los contactos pueden cerrar un circuito de 275 VA. A 125 VCA, los contactos pueden cerrar un circuito de 2.2 amp. Las cargas electromagnéticas de CC no tienen una corriente de entrada al momento del arranque como

las cargas electromagnéticas de CA. La apertura del circuito también es 275 VA porque la corriente es 2.2, nominal o de consumo.

Reinicio de la máquina

Si por ejemplo, se abre una guarda enclavada en una máquina en operación, el interruptor de enclavamiento de seguridad detendrá la máquina. En la mayoría de casos es imperativo que la máquina no se reinicie inmediatamente cuando se cierra la guarda. Una manera común de lograr esto es usar una configuración de arranque con contactor de enclavamiento.

El presionar y soltar el botón de inicio momentáneamente activa la bobina de control del contactor, lo cual cierra los contactos de alimentación eléctrica. Siempre que la alimentación circule a través de los contactos de alimentación, la bobina de control se mantiene activada (enclavada eléctricamente) mediante los contactos auxiliares del contactor, los cuales están mecánicamente vinculados a los contactos de alimentación. Una interrupción de la alimentación principal o del suministro del control resultará en la desactivación de la bobina y en la abertura de los contactos auxiliares y la alimentación principal. El enclavamiento de guarda está cableado al circuito de control del contactor. Esto significa que el reinicio puede lograse sólo cerrando la guarda y luego realizando un encendido con el botón de inicio normal, lo cual restablece el contactor y arranca la máquina.

Los requisitos para situaciones de enclavamiento normales se clarifican en ISO 12100-1 Párrafo 3.22.4 (extracto)

“Cuando la guarda se cierra, pueden quedar operativas las zonas peligrosas de la máquina, pero el cierre de la guarda no inicia por sí solo su operación”.

Muchas máquinas ya tienen contactores simples o dobles que funcionan como se describe anteriormente (o tienen un sistema que logra el mismo resultado). Cuando se acopla un enclavamiento a una maquinaria existente, es importante determinar si la configuración de control de alimentación eléctrica cumple con estos requisitos y tomar las medidas adicionales necesarias.

Funciones de restablecimiento

Los relés de control de seguridad Guardmaster de Allen-Bradley están diseñados con restablecimiento manual monitorizado o restablecimiento automático/manual.

Restablecimiento manual monitorizado

Un restablecimiento manual monitorizado requiere el cierre y abertura de un circuito después que la compuerta se cierra o se restablece el paro de emergencia. Los contactos auxiliares de los contactores de conmutación de alimentación están conectados en serie con un botón pulsador momentáneo. Después que la guarda se abra y se cierre nuevamente, el relé de seguridad no permitirá que se reinicie la máquina hasta que se presione y se suelte el botón de restablecimiento. Cuando esto sucede, el relé de seguridad verifica (es decir, monitoriza)

que ambos contactores estén desactivados y que ambos circuitos de enclavamiento (y por lo tanto las guardas) estén cerrados. Si estas verificaciones son satisfactorias, la máquina puede reiniciarse desde los controles normales. El interruptor de restablecimiento debe ubicarse en un lugar que proporcione una buena visibilidad de la fuente de peligro, de manera que el operador pueda verificar que el área esté despejada antes de la operación.

Restablecimiento automático/manual

Algunos relés de seguridad tienen restablecimiento automático/manual. El modo de restablecimiento manual no se monitoriza y el restablecimiento se produce cuando se presiona el botón. No se detectará un cortocircuito o un atasco en el interruptor de restablecimiento. Alternativamente, la línea de restablecimiento puede conectarse en puente, permitiendo así un restablecimiento automático. Entonces el usuario debe proporcionar otro mecanismo para impedir el inicio de la máquina cuando se cierre la puerta.

Un dispositivo de restablecimiento automático no requiere una acción de conmutación manual, pero después de la desactivación, siempre conducirá una verificación de la integridad del sistema antes de restablecer el mismo. Un sistema de restablecimiento automático no debe confundirse con un dispositivo sin capacidad de restablecimiento. En este último, el sistema de seguridad se habilitará inmediatamente después de la desactivación, pero no habrá una verificación de la integridad del sistema.

Guardas de control

Una guarda de control detiene el funcionamiento de la máquina cuando se abre la guarda e inicia directamente el funcionamiento nuevamente cuando se cierra la guarda. El uso de guardas de control sólo se permite bajo estrictas condiciones ya que cualquier inicio inesperado o incapacidad de parar puede ser extremadamente peligroso. El sistema de enclavamiento debe tener la más alta fiabilidad posible (a menudo se aconseja usar enclavamiento de guarda). El uso de guardas de control SÓLO se puede considerar en maquinaria donde NO EXISTE LA POSIBILIDAD de que un operador o parte de su cuerpo permanezca, o entre en la zona de peligro mientras la guarda está cerrada. La guarda de control debe ser el único acceso al área de peligro.

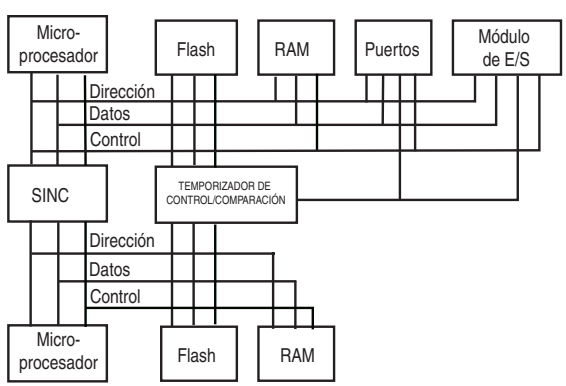
Controladores programables de seguridad

La necesidad de aplicaciones de seguridad flexibles y escalables impulsó el desarrollo de PLCs/controladores de seguridad. Los controladores de seguridad programables proporcionan a los usuarios el mismo nivel de flexibilidad de control en una aplicación de seguridad a la cual están acostumbrados con los controladores programables estándar. Sin embargo existen diferencias extensas entre los PLC estándar y de seguridad. Los PLC de seguridad vienen en varias plataformas para acomodar la capacidad de escalado, los requisitos funcionales y de integración de los sistemas de seguridad complejos.

Hardware

La redundancia de las CPU, la memoria, los circuitos de E/S y los diagnósticos internos son mejoras de los PLC de seguridad que no se requieren en un PLC estándar. Un PLC de seguridad dedica un tiempo significativamente mayor a realizar diagnósticos internos sobre la memoria, las comunicaciones y las E/S. Estas operaciones adicionales se necesitan para alcanzar la certificación de seguridad requerida. El sistema operativo del controlador se hace cargo de esta redundancia y diagnósticos adicionales y los hace transparentes para el programador de modo que los PLC de seguridad programan de una manera muy similar a los PLC estándar.

Los microprocesadores que controlan estos dispositivos realizan diagnósticos internos extensos para asegurar el rendimiento de la función de seguridad. La siguiente figura muestra un ejemplo de diagrama de bloques de un PLC de seguridad. Si bien los controladores basados en microprocesador son ligeramente diferente de una familia a otra, se aplican principios similares para lograr una clasificación de seguridad.



Arquitectura 1oo2D

Se usan múltiples microprocesadores para procesar las E/S, la memoria y las comunicaciones de seguridad. Los circuitos del temporizador de control (watchdog) realizan análisis de diagnósticos. Este tipo de arquitectura se conoce como 1oo2D, porque cualquiera de los dos microprocesadores puede realizar la función de seguridad, y los diagnósticos extensos se realizan para asegurar que ambos microprocesadores estén operando de manera sincronizada.

Además, cada circuito de entrada se prueba internamente repetidas veces cada segundo para asegurar que funcione correctamente. Usted quizás sólo use el paro de emergencia una vez al mes, pero cuando lo haga, el circuito ha sido probado continuamente de modo que el paro de emergencia será detectado correctamente en el interior del PLC de seguridad.

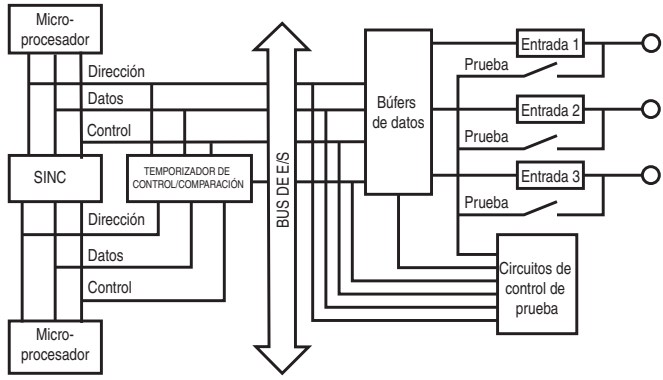


Diagrama de bloques de módulo de entrada de seguridad

Las salidas del PLC de seguridad son electromecánicas o de estado sólido con clasificación de seguridad. Al igual que los circuitos de entrada, los circuitos de salida se prueban múltiples veces cada segundo para asegurar que pueden desactivar la salida. Si uno de los tres falla, la salida es desactivada por los otros dos, y el fallo es reportado por el circuito de monitorización interno.

Cuando se usan dispositivos de seguridad con contactos mecánicos (paros de emergencia, interruptores de compuerta, etc.) el usuario puede aplicar señales de prueba de impulsos para detectar fallos cruzados. Para no usar salidas de seguridad costosas, muchos PLC de seguridad proporcionan salidas de impulsos específicas que pueden conectarse a dispositivos de contactos mecánicos.

Software

Los PLC de seguridad programan de manera similar a los PLC estándar. Todos los diagnósticos adicionales y verificación de errores mencionados anteriormente son realizados por el sistema operativo, por lo tanto el programador no tiene conocimiento de lo que está sucediendo. La mayoría de los PLC de seguridad tendrán instrucciones especiales usadas para escribir el programa para el sistema de seguridad, y estas instrucciones tienden a simular la función de los relés de seguridad homólogos. Por ejemplo, la instrucción de paro de emergencia funciona de manera muy parecida a un MSR 127. Si bien la lógica de estas instrucciones es compleja, los programas de seguridad tienen una apariencia relativamente simple porque el programador simplemente conecta estos bloques juntos. Estas instrucciones, junto con otras instrucciones lógicas, matemáticas, de manipulación de datos, etc., cuentan con certificación de terceros para asegurar que su operación sea coherente con los estándares vigentes.

Los bloques de funciones son métodos predominantes para las funciones de seguridad de programación. Además de los bloques de función y diagramas ladder, los PLC de seguridad

también proporcionan instrucciones de aplicación de seguridad certificadas. Las instrucciones de seguridad certificadas proporcionan un comportamiento específico a la aplicación. Este ejemplo muestra una instrucción de paro de emergencia. Para lograr la misma función en diagramas ladder se requerirían aproximadamente 16 pasos de programa ladder. Puesto que el comportamiento lógico está incorporado en la instrucción E-Stop, la lógica incorporada no tiene que probarse.

Hay bloques de funciones certificados disponibles para hacer interfaz con casi todos los dispositivos de seguridad. Una excepción a esta lista es el borde de seguridad que utiliza tecnología resistiva.

Los PLC de seguridad generan una “firma” que proporciona la capacidad de realizar el seguimiento de los cambios realizados. Esta firma generalmente es una combinación del programa, la configuración de entradas y salidas, y un sello de hora. Al finalizar y validar el programa, el usuario debe registrar esta firma como parte de los resultados de validación para referencia futura. Si el programa necesita modificación, se requiere revalidación y deberá registrarse una nueva firma. El programa también puede bloquearse con una contraseña para evitar cambios no autorizados.

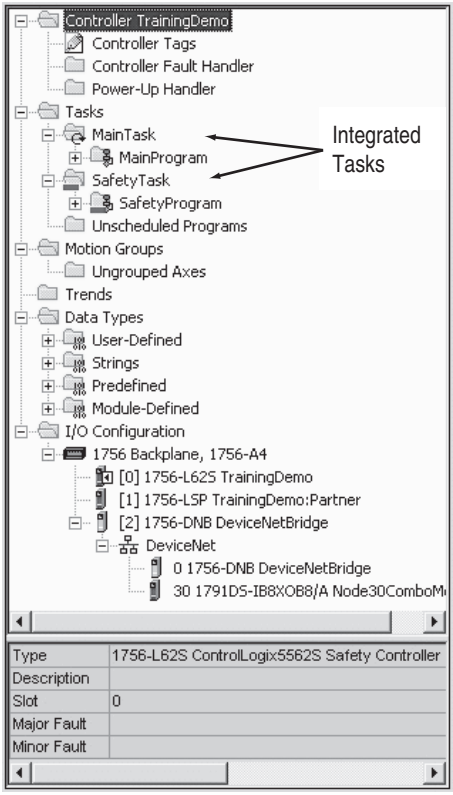
El cableado se simplifica con los programas lógicos comparado con los relés de control de seguridad. A diferencia de cablear a terminales específicos en los relés de control de seguridad, los dispositivos de entrada se conectan a cualquier terminal de entrada y los dispositivos de salida se conectan a cualquier terminal de salida. Luego los terminales son asignados mediante el software.

Controladores de seguridad integrada

Las soluciones de control de seguridad ahora proporcionan una integración completa dentro de una sola arquitectura de control, donde las funciones de seguridad y estándar residen y trabajan juntas. La capacidad de realizar control de movimiento, velocidad, de proceso, de lotes, control secuencial de alta velocidad y seguridad SIL3 en un controlador ofrece ventajas importantes. La integración de los controles de seguridad y estándar ofrece la oportunidad de utilizar herramientas comunes y tecnologías que reducen los costes asociados con el diseño, la instalación, la puesta en marcha y el mantenimiento. La capacidad de utilizar hardware de control común, E/S de seguridad distribuidas o dispositivos en redes de seguridad y dispositivos de interfaz de operador-máquina (HMI) comunes reducen los costes de adquisición y mantenimiento así como también el tiempo de desarrollo. Todas estas características aumentan la productividad y la velocidad relacionada con la resolución de problemas, y reducen los costes de formación técnica gracias a la homogeneidad.

El siguiente diagrama muestra un ejemplo de la integración del control y la seguridad. Las funciones de control estándar no relacionadas a la seguridad residen en la tarea principal. Las funciones relacionadas con la seguridad residen en la tarea de seguridad.

Todas las funciones estándar y relacionadas a la seguridad están aisladas unas de otras. Por ejemplo, los tags de seguridad pueden ser leídos directamente por la lógica estándar. Los tags de seguridad pueden intercambiarse entre los controladores GuardLogix mediante EtherNet, ControlNet o DeviceNet. Los datos de tags de seguridad pueden ser leídos directamente por dispositivos externos, interfaces de máquina-operador (HMI), ordenadores personales (PC) y otros controladores.



1. Los tags estándar y la lógica se comportan igual que los de ControlLogix.

2. Datos de tags estándar, programa o dispositivos al alcance del controlador, HMI, PC, otros controladores, etc.

3. Como controlador integrado, GuardLogix proporciona la capacidad de mover (asignar) datos de tags estándar a tags de seguridad para uso dentro de la tarea de seguridad. El objeto de ello es proporcionar a los usuarios la capacidad de leer información de estado desde el lado estándar de GuardLogix. Estos datos no deben usarse para controlar directamente una salida de seguridad.

4. Los tags de seguridad pueden ser leídos directamente por la lógica estándar.

5. Los tags de seguridad pueden ser escritos o leídos por la lógica de seguridad.

6. Los tags de seguridad pueden intercambiarse entre los controladores GuardLogix mediante EtherNet.

7. Los datos de tags de seguridad, del programa o de los dispositivos al alcance del controlador pueden ser leídos por dispositivos externos, HMI, PC u otros controladores, etc. Tome nota de que una vez que se leen estos datos, se consideran datos estándar, no datos de seguridad.

Redes de seguridad

Las redes de comunicación de la planta tradicionalmente han proporcionado a los fabricantes la capacidad de mejorar la flexibilidad, aumentar los diagnósticos, aumentar las distancias, reducir los costes de instalación y cableado, facilitar el mantenimiento y en general mejorar la productividad de sus operaciones de fabricación. Estas mismas motivaciones también están

impulsando la implementación de redes de seguridad industriales. Estas redes de seguridad permiten a los fabricantes distribuir E/S de seguridad y dispositivos de seguridad alrededor de su maquinaria mediante un solo cable de red, para reducir los costes de instalación a la vez que se mejoran los diagnósticos y se habilitan sistemas de seguridad de mayor complejidad. También permiten comunicaciones seguras entre los PLC de seguridad/controladores y permiten a los usuarios distribuir su control de seguridad entre varios sistemas inteligentes.

Las redes de seguridad no eliminan los errores de comunicación. Las redes de seguridad tienen mayor capacidad de detectar errores de transmisión y luego permitir que los dispositivos de seguridad realicen las acciones apropiadas. Los errores de comunicación que se detectan incluyen: inserción de mensajes, pérdida de mensajes, corrupción de mensajes, retardo de mensajes, repetición de mensajes y secuencia incorrecta de mensajes.

Para la mayoría de aplicaciones, cuando se detecta un error el dispositivo entra en un estado desactivado conocido, generalmente llamado “estado de seguridad”. La entrada de seguridad o el dispositivo de seguridad es responsable de detectar estos errores de comunicación y luego entrar en el estado de seguridad si corresponde.

Las redes de seguridad de versiones anteriores estaban vinculadas a un tipo de medio físico o a un esquema de acceso a medio físico, por lo tanto los fabricantes tenían que usar cables específicos,tarjetas de interfaz de red, routers, bridges, etc., que también se convertían en parte de la función de seguridad. Estas redes estaban limitadas en el sentido que sólo aceptaban comunicación entre dispositivos de seguridad. Esto significaba que los fabricantes tenían que usar dos o más redes para su estrategia de control de máquina (una red para el control estándar y otra para el control relacionado a la seguridad), lo cual aumentaba los costes de instalación, formación técnica y piezas de repuesto.

Las redes de seguridad modernas permiten que un solo cable de red se comunique con los dispositivos de control de seguridad y estándar, El protocolo CIP (protocolo industrial común) Safety es un protocolo estándar abierto publicado por ODVA (Open DeviceNet Vendors Association) que permite comunicaciones de seguridad entre dispositivos de seguridad en las redes DeviceNet, ControlNet y EtherNet/IP. Puesto que CIP Safety es una extensión del protocolo CIP estándar, los dispositivos de seguridad y los dispositivos estándar pueden residir en la misma red. Los usuarios también pueden hacer conexión en puente entre redes que contienen dispositivos de seguridad, lo cual les permite subdividir los dispositivos de seguridad para realizar ajustes finos en los tiempos de respuesta de seguridad o simplemente facilitar la distribución de los dispositivos de seguridad. Puesto que el protocolo de seguridad es únicamente responsabilidad de los dispositivos finales (PLC de seguridad/controlador, modulo de E/S de seguridad, componente de seguridad), se usan cables estándar, tarjetas de interfaz de red, routers y bridges, lo cual elimina accesorios especiales de conexión en red y permite apartar estos dispositivos de la función de seguridad.

Dispositivos de salida

Relés de control de seguridad y contactores de seguridad

Los relés de control y los contactores se usan para desconectar la alimentación eléctrica del accionador. Se añaden características especiales a los relés de control y contactores para proporcionar la clasificación de seguridad.

Se usan contactos normalmente cerrados unidos mecánicamente para informar el estado de los relés de control y contactores al dispositivo lógico. El uso de contactos unidos mecánicamente ayuda a asegurar la función de seguridad. Para cumplir con los requisitos de los contactos mecánicamente unidos, los contactos normalmente cerrados y normalmente abiertos no pueden estar en el estado cerrado simultáneamente. La normativa IEC 60947-5-1 define los requisitos para los contactos mecánicamente unidos. Si los contactos normalmente abiertos se fueran a soldar, los contactos normalmente cerrados se abrirían por lo menos 0.5 mm. Por el contrario, si los contactos normalmente cerrados se fueran a soldar, entonces los contactos normalmente abiertos permanecerían abiertos.

Los sistemas de seguridad sólo deben arrancar en lugares específicos. Los relés de control y los contactores estándar permiten que se actue sobre el contactor manualmente. En los dispositivos de seguridad, no se puede actuar manualmente ya que están protegidos.

En los relés de control de seguridad el contacto normalmente cerrado es de guía forzada. Los contactores de seguridad utilizan un bloque de contactos auxiliares para ubicar los contactos mecánicamente unidos. Si el bloque de contactos se cayera de la base, los contactos mecánicamente unidos permanecerían cerrados. Los contactos mecánicamente unido están permanentemente adheridos al relé de control de seguridad o contactor de seguridad.

En los contactores de mayor tamaño, un bloque de contactos auxiliares es insuficiente para reflejar con precisión el estado del separador más ancho. Se usan contactos en espejo mostrados en la Figura 4.81 y ubicados en cualquiera de los lados del contactor.

El tiempo de desconexión de los relés de control o contactores desempeña un papel en el cálculo de la distancia de seguridad. A menudo, un supresor de sobretensión se coloca en la bobina para aumentar la vida útil de los contactos que accionan la bobina. Para las bobinas activadas por CA, el tiempo de desconexión no se ve afectado. Para las bobinas activadas por CC, el tiempo de desconexión aumenta. El aumento depende del tipo de supresión seleccionado.

Los relés de control y contactores están diseñados para conmutar grandes cargas, desde 0,5 A hasta más de 100 A. El sistema de seguridad opera con baja corriente. La señal de realimentación generada por el dispositivo lógico del sistema de seguridad puede estar en el orden de unos pocos miliamperios hasta decenas de miliamperios, generalmente a 24 VCC. Los relés de control de seguridad y los contactores de seguridad usan contactos bifurcados con recubrimiento de oro para conmutar de una manera fiable esta baja corriente.

Protección contra sobrecarga

Los estándares eléctricos requieren protección contra sobrecarga de los motores. Los diagnósticos provistos por el dispositivo de protección contra sobrecarga mejoran no sólo la seguridad del equipo sino también la seguridad del operador. Las tecnologías disponibles hoy en día pueden detectar condiciones de fallo como una sobrecarga, pérdida de fase, fallo de tierra, bloqueo, atasco, baja carga, desequilibrio de corriente y sobretemperatura. El detectar y comunicar condiciones anormales antes del disparo ayuda a mejorar el tiempo productivo y ayuda a evitar condiciones peligrosas no previstas para los operadores y el personal de mantenimiento

Variadores y servovariadores

Los variadores y servovariadores con clasificación de seguridad pueden usarse para evitar el riesgo de movimiento mecánico para lograr un paro de seguridad así como un paro de emergencia.

Los variadores de CA logran la clasificación de seguridad con canales redundantes para desconectar la alimentación eléctrica al circuito de control de la compuerta. Un canal es la señal de habilitación, una señal de hardware que elimina la señal de entrada del circuito de control de compuerta. El segundo canal es un relé con guía positiva que elimina el suministro de alimentación eléctrica del circuito de control de la compuerta. El relé con guía positiva también proporciona una señal de estado de vuelta al sistema lógico. Este enfoque redundante permite que el variador de seguridad se aplique en circuitos de paro de emergencia sin necesidad de un contactor.

El servovariador logra un resultado de manera similar a los variadores de CA mediante señales de seguridad redundantes usadas para lograr la función de seguridad. Una señal interrumpe la alimentación eléctrica del variador al circuito de control de compuerta. Una segunda señal interrumpe la alimentación eléctrica a la fuente de alimentación eléctrica del circuito de control de compuerta. Se usan dos relés con guía positiva para eliminar las señales y proporcionar también realimentación al dispositivo lógico de seguridad.

Sistemas de conexión

Los sistemas de conexión añaden valor al reducir los costes de instalación y mantenimiento de los sistemas de seguridad. Los diseños deben tener en cuenta aspectos tales como una solo canal, dos canales, dos canales con indicación y múltiples tipos de dispositivos.

Cuando se necesita una conexión en serie de enclavamientos de dos canales, un bloque de distribución puede simplificar la instalación. Con la clasificación IP67, estos tipos de cajas pueden montarse en la máquina en lugares remotos. Cuando se requiere un conjunto diverso de dispositivos, puede usarse una caja ArmorBlock Guard I/O. Las entradas pueden ser configuradas mediante software para aceptar varios tipos de dispositivos.

Cálculo de la distancia de seguridad

La piezas peligrosas deben estar en un estado de seguridad antes de que el operador entre en contacto con ellas Para realizar el cálculo de la distancia de seguridad, existen dos grupos de estándares usados comúnmente. En este capítulo, estos estándares se agrupan de la siguiente manera:

ISO EN: (ISO 13855 y EN 999)

US CAN (ANSI B11.19, ANSI RIA R15.06 y CAN/CSA Z434-03)

Fórmula

La distancia de seguridad mínima depende del tiempo requerido para procesar el comando de Paro y cuánto puede penetrar el operador en la zona de detección antes de ser detectado. La fórmula usada en todo el mundo tiene el mismo formato y requisitos. Las diferencias son los símbolos usados para representar las variables y las unidades de medición.

Las fórmulas son:

ISO EN: $S = K \times T + C$

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

Donde: Ds y S son la distancia segura mínima de la zona de peligro hasta el punto de detección más cercano

Direcciones de aproximación

Al considerar el cálculo de la distancia de seguridad donde se usa una barrera de seguridad o un escáner de área, debe tenerse en cuenta la aproximación al dispositivo de detección. Se consideran tres tipos de aproximación:

Normal – una aproximación perpendicular al plano de detección

Horizontal – una aproximación paralela al plano de detección

En ángulo – una aproximación en ángulo a la zona de detección.

Constante de velocidad

K es una constante de velocidad. El valor de la constante de velocidad depende de los movimientos del operador (por ej., velocidades de las manos, velocidades de caminar y longitudes de las zancadas al caminar). Este parámetro se basa en datos de investigación que muestran que es razonable suponer una velocidad de la mano de 1600 mm/seg (63 pulg./s) de un operador mientras el cuerpo está estacionario. Deben tenerse en cuenta las circunstancias de la aplicación real. Como guía general, la velocidad de aproximación variará

de 1600 mm/s (63 pulg./s) a 2500 mm/seg (100 pulg./s). La constante de velocidad apropiada debe ser determinada por la evaluación de riesgos.

Tiempo de paro

T representa el tiempo de paro total del sistema. El tiempo total en segundos comienza desde el inicio de la señal de paro hasta el paro de la pieza peligrosa. Este tiempo puede desglosarse a sus partes incrementales (Ts, Tc, Tr y Tbm) para facilitar el análisis. Ts representa el tiempo de paro en el peor de los casos de la máquina/equipo Tc representa el tiempo de paro en el peor de los casos del sistema de control Tr representa el tiempo de respuesta del dispositivo de protección, inclusive su interfaz. Tbm representa el tiempo de paro adicional permitido por el monitor del freno antes de que detecte deterioro del tiempo de paro más allá de los límites predeterminados por los usuarios finales. Tbm se usa para prensas mecánicas de piezas con revoluciones. Ts + Tc + Tr generalmente son medidos por un dispositivo de medición de tiempo de paro si los valores son desconocidos.

Factores de penetración de profundidad

Los factores de penetración de profundidad son representados por los símbolos C y Dpf. Es el máximo recorrido hacia el peligro antes de la detección por parte del dispositivo de protección. Los factores de penetración de profundidad cambiarán según el tipo de dispositivo y la aplicación. Debe verificarse el estándar apropiado para determinar el mejor factor de penetración de profundidad. Para una aproximación normal a una barrera de seguridad o escáner de área, cuya sensibilidad objeto es menos de 64 mm (2.5 pulg.), los estándares de ANSI y los canadienses usan:

Dpf = 3,4 x (sensibilidad objeto – 6,875 mm), pero no menos de cero.

Para una aproximación normal a una barrera de seguridad o escáner de área, cuya sensibilidad objeto es menos de 40 mm (1.57 pulg.), los estándares de ISO y EN usan:

C = 8 x (sensibilidad objeto – 14 mm), pero no menos de 0.

Estas dos fórmulas tienen un punto de cruce a 19,3 mm. Para una sensibilidad de objeto menor de 19 mm, la aproximación US CAN es más restrictiva, puesto que la barrera de seguridad o el escáner de área debe colocarse más alejado de la pieza peligrosa. Par sensibilidades de objetos de más de 19,3 mm, el estándar ISO EN es más restrictivo. Los constructores de máquinas que desean construir una máquina para uso en todo el mundo, deben usar las condiciones en el peor de los casos de ambas ecuaciones.

Aplicaciones de aproximación horizontal

Cuando se usan sensibilidades de objetos más grandes, los estándares US CAN e ISO EN difieren ligeramente en el factor de penetración de profundidad y en la sensibilidad del objeto. La Figura 5.2 resume las diferencias. El valor de ISO EN es 850 mm donde el valor de US CAN es 900 mm. Los estándares también difieren en la sensibilidad del objeto. Donde el estándar ISO EN permite 40 a 70 mm, el estándar US CAN permite hasta 600 mm.

Aplicaciones de aproximación vertical

Ambos estándares aceptan que la altura mínima del haz más bajo debe ser de 300 mm, pero difieren con respecto a la altura mínima del haz más alto. El ISO EN establece 900 mm, mientras que el US CAN establece 1200 mm. El valor para el haz más alto parece ser irrelevante. Al considerar una aplicación de alcanzar al otro lado, la altura del haz más alto tendrá que ser mucho mayor para aceptar a un operador en posición parada. Si el operador puede alcanzar por arriba del plano de detección, entonces se aplican los criterios de alcanzar por arriba.

Uno o varios haces

Los haces individuales o múltiples son definidos en más detalle por los estándares ISO EN. Las siguientes figuras muestran las alturas “prácticas” de múltiples haces arriba del suelo. La penetración de profundidad es 850 mm para la mayoría de los casos y 1200 mm para el uso de haz único. En comparación, la aproximación US CAN toma esto en consideración mediante los requisitos de alcanzar al otro lado. El pasar por encima, por debajo o alrededor de uno o múltiples haces siempre debe tenerse en consideración.

Número de haces	Altura por encima del piso (mm)	C (mm)
1	750	1200
2	400, 900	850
3	300, 700, 1100	850
4	300, 600, 900, 1200	850

Cálculos de distancia

Para la aproximación normal a las barreras de seguridad, el cálculo de la distancia de seguridad para ISO EN y US CAN es parecido, pero existen diferencias. Para la aproximación normal a las cortinas de luz vertical donde la sensibilidad del objeto es un máximo de 40 m, la aproximación ISO EN requiere dos pasos. Primero, calcular S usando 2000 para la velocidad constante.

S = 2000 x T + 8 x (d -1 4)

La distancia mínima a la que puede estar S es 100 mm.

Un segundo paso puede usarse cuando la distancia es mayor que 500 mm. Entonces, el valor de K puede reducirse a 1600. Cuando se usa K = 1600, el valor mínimo de S es 500 mm.

La aproximación de US CAN utiliza un método de un paso: Ds = 1600 x T * Dpf

Esto causa diferencias mayores del 5% entre los estándares, cuando el tiempo de respuesta es menor que 560 ms.

Aproximaciones en ángulo

La mayoría de aplicaciones de barreras de seguridad y escáneres se montan en plano vertical (aproximación normal) u horizontal (aproximación paralela). Estos montajes no se consideran en ángulo si se encuentran dentro de ±5° del diseño previsto. Cuando el ángulo exceda el valor de ±5°, deberán considerarse los riesgos potenciales (por ej., distancia más corta) de aproximaciones previsibles. En general, los ángulos de más de 30° con respecto al plano de referencia (por ej., el suelo) deben considerarse normales y los ángulos de menos de 30 deben considerarse paralelos.

Alfombras de seguridad

Con los tapetes de seguridad, la distancia de seguridad debe tener en cuenta el ritmo de los pasos y la zancada de los operadores. Suponiendo que el operador está caminando y los tapetes de seguridad están instalados sobre el suelo. El primer paso que da el operador sobre el tapete es un factor de penetración de profundidad de 1200 mm o 48 pulg. Si el operador debe subirse sobre una plataforma, entonces el factor de penetración de profundidad puede reducirse por un factor del 40% de la altura del paso.

Ejemplo

Ejemplo: Un operador usa una aproximación normal a una barrera de seguridad de 14 mm, que está conectada a un relé de control de seguridad, el cual está conectado a un contactor activado a CC con un supresor de diodo. El tiempo de respuesta del sistema de seguridad, Tr, es 20 + 15 + 95 = 130 ms. El tiempo de paro de la máquina, Ts+Tc, es 170 ms. No se usa monitor de freno. El valor Dpf es 1 pulgada y el valor C es cero. El cálculo sería como se indica a continuación

Dpf = 3.4 (14 – 6.875) = 1 pulg. (24,2 mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0.17 + 0.13 + 0) + 1
Ds = 63 x (0.3) + 1
Ds = 18,9 + 1
Ds = 19.9 pulg. (505 mm)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18.9 pulg.)

Por lo tanto, la distancia de seguridad mínima a la que la barrera de seguridad de seguridad debe instalarse de la pieza de peligro es 20 pulgadas ó 508 mm, para una máquina que se use en cualquier lugar del mundo.

Prevención de una puesta en marcha intempestiva

Muchos estándares abarcan la prevención de una activación inesperada. Algunos ejemplos son ISO 14118, EN 1037, ISO 12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 y AS 4024.1603. Estos estándares tienen un tema común: el método primario de evitar una activación inesperada es desconectar la energía del sistema y bloquear el sistema en estado desactivado. El propósito es permitir el ingreso seguro de las personas a las zonas peligrosas de una máquina.

Bloqueo de seguridad

Las nuevas máquinas deben construirse con dispositivos de aislamiento de la energía bloqueables. Los dispositivos se aplican a todos los tipos de energía, tales como eléctrica, hidráulica, neumática, de gravedad y láser. Bloqueo significa aplicar un bloqueo a un dispositivo aislador de energía. El bloqueo sólo debe ser retirado por su propietario o por un supervisor bajo condiciones controladas. Cuando varias personas deben trabajar en la máquina, cada persona debe aplicar sus bloqueos a los dispositivos de aislamiento de energía. Cada bloque debe ser identificable para su propietario.

En los EE.UU. el etiquetado de seguridad es una alternativa al bloqueo para las máquinas antiguas si nunca se instaló un dispositivo bloqueable. En este caso la máquina se desactiva y se coloca una etiqueta para advertir a todo el personal que no arranque la máquina mientras el portador de la etiqueta está trabajando en la máquina. A partir de 1990, las máquinas modificadas deben actualizarse para incluir un dispositivo aislador de energía bloqueable.

Un dispositivo aislador de energía es un dispositivo mecánico que evita físicamente la transmisión o liberación de energía. Estos dispositivos pueden ser un interruptor automático, un desconectador, un interruptor operado manualmente, una combinación de conector/socket o una válvula de operación manual. Los dispositivos de aislamiento eléctrico deben desconectar las fases de alimentación de suministro sin conexión a tierra y ningún polo deberá operar independientemente.

El propósito del bloqueo y etiquetado de seguridad es evitar un arranque inesperado de la máquina. Un arranque inesperado puede ser resultado de varias causas: Un fallo del sistema de control; una acción inapropiada en un control de arranque, sensor, contactor o válvula; una restauración de la alimentación eléctrica después de una interrupción o alguna otra influencia interna o externa. Después de realizar el procedimiento de bloqueo o etiquetado de seguridad, debe verificarse la disipación de la energía.

Sistemas de aislamiento de seguridad

Los sistemas de aislamiento de seguridad ejecutan una desactivación ordenada de una máquina y también proporcionan un método fácil de bloquear la alimentación eléctrica de una máquina. Este método funciona bien para sistemas de fabricación y máquinas de mayor tamaño, especialmente cuando varias fuentes de energía están ubicadas a nivel de entresuelo o en lugares distantes.

Interruptores de corte en carga

Para el aislamiento local de dispositivos eléctricos es posible colocar interruptores justo antes del dispositivo que necesita aislarse y bloquearse. Los interruptores de carga referencia 194E son un ejemplo de un producto con capacidad de aislamiento y bloqueo.

Sistemas con atrapamiento de llave

Los sistemas con atrapamiento de llave son otro método para implementar un sistema de bloqueo. Muchos sistemas con atrapamiento de llave comienzan con un dispositivo aislador de energía. Cuando el interruptor es desactivado por la llave “primaria”, se desconecta la energía eléctrica a la máquina para fases de alimentación sin conexión a tierra simultáneamente. La llave primaria puede retirarse y llevase a un lugar donde se requiera acceso a la máquina. La Figura 6.4 muestra un ejemplo del sistema más básico, un interruptor de aislamiento y un bloqueo de acceso a compuerta. Es posible añadir varios componentes para configuraciones de bloqueo más complejas.

Medidas alternativas al bloqueo

El bloqueo y etiquetado de seguridad deben usarse durante las tareas de servicio o mantenimiento de las máquinas. La protección incluye intervenciones de máquinas durante las operaciones normales de producción. La diferencia entre las operaciones de servicio/mantenimiento y las operaciones normales de producción no siempre es clara.

Algunos ajustes menores y tareas de servicio que se llevan a cabo durante las operaciones de producción normales, no necesariamente requieren que se bloquee la máquina. Algunos ejemplos son carga y descarga de materiales, cambios y ajustes menores en las herramientas, niveles de lubricación de servicio y retirar el material de desecho. Estas tareas deben ser rutinarias, repetitivas e integrales al uso del equipo de producción, y el trabajo se realizará usando medidas alternativas, tales como medidas eficaces de protección. Las medidas de protección incluyen dispositivos como guardas de enclavamiento, barreras de seguridad y alfombras de seguridad. Con la lógica de seguridad y los dispositivos de salida apropiados, los operadores pueden acceder de manera segura a las zonas peligrosas de la máquina durante las tareas de producción normales y de servicio de mantenimiento menor.

Estructura de los sistemas de control con fines de seguridad

Introducción

¿Qué es un sistema de control con fines de seguridad (conocido por la abreviatura SRCS)? Es la parte del sistema de control de una máquina que evita que ocurra una condición peligrosa. Puede ser un sistema dedicado separado o puede estar integrado con el sistema de control normal de la máquina.

Su complejidad puede variar desde un sistema simple, tal como un interruptor de enclavamiento de puerta de guarda e interruptor de paro de emergencia conectados en serie, a la bobina de control de un contactor de alimentación eléctrica, hasta un sistema compuesto que comprende dispositivos simples y complejos que se comunican a través de software y hardware.

Los sistemas de control con fines de seguridad están diseñados para realizar funciones de seguridad. Los SRCS deben continuar operando correctamente en todas las condiciones previsibles. Por lo tanto ¿qué es una función de seguridad; cómo diseñamos un sistema que logre esto, y cuando lo hayamos hecho, cómo hacemos una demostración?

Función de seguridad

Una función de seguridad es implementada por las partes relacionadas a la seguridad del sistema de control de la máquina para lograr o mantener el equipo bajo control en un estado de seguridad con respecto a un peligro específico. Un fallo de la función de seguridad puede resultar en un aumento inmediato de los riesgos de usar el equipo, es decir, una condición peligrosa.

Una máquina debe tener por lo menos un “peligro”, de lo contrario no es una máquina. Una “condición peligrosa” es cuando una persona es expuesta a un peligro. Una condición peligrosa no implica que la persona sufrirá daño. La persona expuesta puede tener capacidad de reconocer el peligro y evitar ser lesionada. La persona expuesta podría no ser capaz de reconocer el peligro, o el peligro puede ser causado por un arranque inesperado. La tarea principal del diseñador del sistema de seguridad es evitar condiciones peligrosas y evitar un arranque inesperado.

La función de seguridad a menudo puede describirse con requisitos de múltiples partes. Por ejemplo, la función de seguridad iniciada por una guarda de enclavamiento tiene tres partes:

1. las piezas peligrosas protegidas por la guarda no pueden operar hasta que la guarda esté cerrada;

2. abrir la guarda causará que la pieza peligrosa se detenga si está operativa al momento de la apertura; y

3. el cierre de la guarda no hace que vuelva a arrancar la pieza peligrosa protegida por la guarda.

Al establecer la función de seguridad para una aplicación específica, la palabra “pieza peligrosa” debe cambiarse al nombre de la pieza peligrosa especifica. El peligro no debe confundirse con los resultados del peligro. La trituración, los cortes y las quemaduras son resultados de un peligro. Un ejemplo de una pieza peligrosa es un motor, ariete, cuchilla, soplete, bomba, láser, robot, efector final, solenoide, válvula, otro tipo de accionador o un peligro mecánico que implica gravedad.

Al discutir los sistemas de seguridad, se utiliza la frase “al imponer o antes de que se imponga una demanda sobre una función de seguridad”. ¿Qué es una demanda impuesta sobre una función de seguridad? Algunos ejemplos de demandas impuestas sobre la función de seguridad son la abertura de una guarda de enclavamiento, la interrupción de una cortina de luz, pisar un tapete de seguridad o presionar un paro de emergencia. Un operador demanda que se detenga la pieza peligrosa o que permanezca desenergizada si ya está detenida.

Las piezas con fines de seguridad del sistema de control de la máquina ejecutan la función de seguridad. La función de seguridad no es ejecutada por un solo dispositivo, por ejemplo solamente la guarda. El enclavamiento de la guarda envía un comando a un dispositivo lógico, el cual a su vez, inhabilita un accionador. La función de seguridad se inicia con el comando y termina con la implementación.

El sistema de seguridad debe diseñarse con un nivel de integridad acorde con los riesgos de la máquina. Los riesgos más altos requieren niveles de integridad mayores para asegurar el rendimiento de la función de seguridad. Los sistemas de seguridad de la máquina pueden categorizarse según el propósito de su diseño y la capacidad de asegurar el rendimiento de la función de seguridad.

Categorías de los sistemas de control

La siguiente descripción de categorías se basa en el estándar ISO 13849-1:1999, que equivale a EN 954-1:1996. En 2006, ISO 13849-1 se modificó de manera significativa para armonizar con IEC 62061 e IEC 61508, cuyo uso se prefiere para sistemas de seguridad altamente complejos. La versión 2006 de ISO 13849-1 continúa utilizando categorías de rendimiento de seguridad; las categorías son consideradas la “estructura” o la “arquitectura” de los SRCS. Información adicional acerca de los componentes del diseño del sistema complementa esta “estructura” para proporcionar una clasificación de “nivel de rendimiento”. La descripción de categorías aquí corresponde a las revisiones de 1999 y 2006 del estándar ISO 13849-1.

El estándar ISO 13849-1 “Piezas con fines de seguridad de los sistemas de control, Parte 1, Principios generales de diseño” establece un “lenguaje” de cinco categorías de referencia y descripción del rendimiento de los SRCS.

> **Nota 1:** La Categoría B por sí misma no tiene medidas especiales de seguridad, pero forma la base para las otras categorías.

Nota 2: En caso de múltiples fallos causados por una causa común o como consecuencia inevitable del primer fallo, éstos deben contarse como un solo fallo.

Nota 3: La revisión de fallos puede limitarse a dos fallos combinados si se justifica, pero los circuitos complejos (por ej., circuitos de microprocesador) pueden requerir la consideración de más fallos combinados.

Entonces, ¿cómo se decide qué categoría se necesita? El proceso de evaluación de riesgos debe conducir a la categoría apropiada. Para traducir estos requisitos a una especificación de diseño de sistema, tiene que haber una interpretación de los requisitos básicos.

Es un error común creer que la categoría 1 proporciona la mínima protección y que la categoría 4 proporciona la máxima. Éste no es el razonamiento con el que se crearon las categorías. Estas se han diseñado como puntos de referencia que describen el rendimiento funcional de diferentes métodos de control relacionado con la seguridad y las partes que lo constituyen.

La Categoría 1 tiene el propósito de PREVENIR fallos. Esto se logra utilizando principios de diseño, componentes y materiales adecuados. La simplicidad del principio y el diseño complementado con características estables y predecibles del material, son las claves de esta categoría.

Las categorías 2, 3 y 4 requieren que si un fallo no se puede evitar, éste se debe DETECTAR y debe realizarse la acción apropiada.

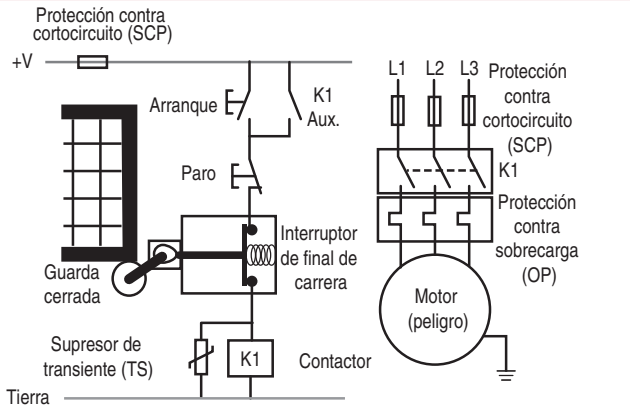
La redundancia, la diversidad y la monitorización son las claves de estas categorías. La redundancia es la duplicación de la misma técnica. Diversidad es usar dos técnicas diferentes. Monitorización es verificar el estado de los dispositivos y luego tomar la acción apropiada según los resultados del estado. El método usual (pero no el único) de monitorización es duplicar las funciones críticas de seguridad y comparar la operación.

Resumen de requisitos	Comportamiento del sistema
CATEGORÍA B (vea la nota 1) Las piezas relacionadas con la seguridad de los sistemas de control de máquina y/o su equipo protector, así como sus componentes, se diseñarán, construirán, seleccionarán, ensamblarán y combinarán de acuerdo con los estándares pertinentes, de manera que puedan soportar las influencias previstas. Se aplicarán los principios de seguridad básicos.	Cuando ocurre un fallo, éste puede causar la pérdida de la función de seguridad.
CATEGORÍA 1 Los requisitos de la categoría B se aplican junto con el uso de componentes de seguridad y principios de seguridad debidamente comprobados.	Como se describió para la categoría B, pero con una fiabilidad más alta de la función de seguridad. (Cuanta más alta la fiabilidad, menor la probabilidad de un fallo).
CATEGORÍA 2 Se aplican los requisitos de la categoría B y el uso de principios de seguridad debidamente comprobados. El sistema de control de la máquina verificará la(s) función(es) de seguridad al momento de la puesta en marcha de la máquina y periódicamente. Si se detecta un fallo se iniciará un estado de seguridad o, si esto no es posible, se emitirá una advertencia.	La verificación detecta la pérdida de la función de seguridad. La ocurrencia de un fallo puede causar la pérdida de la función de seguridad entre los intervalos de verificación.
CATEGORÍA 3 (vea las notas 2 y 3) Se aplican los requisitos de la categoría B y el uso de principios de seguridad debidamente comprobados. El sistema estará diseñado de manera que un fallo en cualquiera de sus piezas no cause la pérdida de la función de seguridad. Cuando sea práctico, se detectará un fallo individual.	Cuando ocurre el fallo, la función de seguridad siempre se ejecuta. Se detectarán algunos fallos, pero no todos. Una acumulación de fallos no detectados puede causar la pérdida de la función de seguridad.
CATEGORÍA 4 (vea las notas 2 y 3) Se aplican los requisitos de la categoría B y el uso de principios de seguridad debidamente comprobados. El sistema se diseñará de manera que un solo fallo en alguna de sus partes no conduzca a la pérdida de la función de seguridad. El fallo individual se detecta al momento de la siguiente demanda sobre la función de seguridad o antes de ésta. Si esta detección no es posible, entonces una acumulación de fallos no causará una pérdida de la función de seguridad.	Cuando ocurren fallos, la función de seguridad siempre se ejecuta. Los fallos se detectarán a tiempo para evitar la pérdida de las funciones de seguridad.

Categoría B

La Categoría B proporciona los requisitos básicos de cualquier sistema de control; ya sea un sistema de control con fines de seguridad o no relacionado a la seguridad. Un sistema de control debe funcionar en su entorno esperado. El concepto de fiabilidad proporciona una base para los sistemas de control ya que la fiabilidad se define como la probabilidad de que un dispositivo realice su función prevista durante un intervalo especificado y bajo condiciones previstas. Si bien tenemos un sistema que cumple con nuestras metas de fiabilidad, sabemos que los sistemas fallarán en algún momento. El diseñador del sistema de seguridad necesita saber si el sistema fallará y causará un peligro o si fallará y entrará a un estado de seguridad. La pregunta es, "¿cómo se desempeñará el sistema en la presencia de fallos?" Comenzando con este concepto, ¿cuáles principios deben seguirse para guiar el diseño del sistema? La categoría B requiere la aplicación de los principios de seguridad básicos. El estándar ISO 13849-2 indica los principios de seguridad básicos para los sistemas eléctricos, neumáticos, hidráulicos y mecánicos. Los principios eléctricos se resumen de la siguiente manera:

- Selección, combinación, configuraciones, ensamblaje e instalación correctos (es decir, según las instrucciones del fabricante)
- Compatibilidad de componentes con voltajes y corrientes
- Resistencia de las condiciones ambientales
- Uso del principio de desactivación
- Supresión de transitorios
- Reducción del tiempo de respuesta
- Protección contra un arranque inesperado
- Instalación segura de dispositivos de entrada (por ej., montaje de dispositivos de enclavamiento)
- Protección del circuito de control (según NFPA 79 y IEC 60204-1)
- Correcta conexión equipotencial de protección

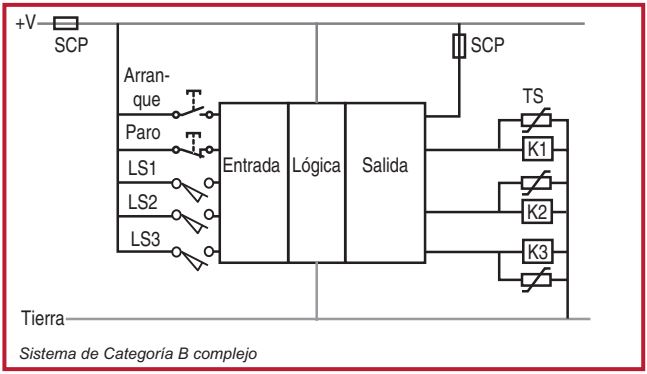


Sistema de Categoría B simple

Aquí se muestra un ejemplo de un sistema de Categoría B. La guarda está enclavada con un interruptor de final de carrera en modo negativo (accionado por resorte). La protección contra cortocircuito y sobrecarga se proporciona para cumplir con los requisitos del estándar eléctrico para

protección del circuito de control. La supresión de transitorios se usa para ayudar a evitar la soldadura de contactos cuando se desactiva la bobina del contactor. Se usa el principio de desenergización: el enclavamiento de la guarda apaga el motor. Los componentes deben seleccionarse e instalarse para cumplir con las condiciones ambientales previsibles y los requisitos de corriente y de voltaje. Tenga en cuenta que no se aplica ninguna medida de seguridad según la Categoría B, por lo tanto quizás se requieran medidas adicionales.

Presione el botón Start con la guarda cerrada para activar el motor, lo cual simboliza el peligro. Cuando el contactor K1 se cierra, un contacto auxiliar mantiene el circuito y puede soltarse el botón Start. Presione el botón Stop o abra la guarda para apagar el motor. Soltar el botón Stop o cerrar la guarda no causan que el motor vuelva a arrancar.



Sistema de Categoría B complejo

Aquí se muestra un sistema complejo que cumple con los requisitos de la Categoría B. Aquí múltiples dispositivos de detección (interruptores de final de carrera) y botones pulsadores están conectados al módulo de entrada de un controlador lógico programable (PLC). Múltiples accionadores están conectados al módulo de salida. Un módulo lógico que utiliza software determina cuáles salidas se activan o desactivan en respuesta al estado de los dispositivos de detección.

¿Cómo sabemos que estos circuitos cumplen con la Categoría B? Primero, el diseñador debe seleccionar, instalar y ensamblar el producto siguiendo las instrucciones del fabricante. Estos dispositivos deben funcionar dentro de las clasificaciones de voltaje y corriente previstas. Las condiciones ambientales previstas, como compatibilidad electromagnética, vibración, choque, contaminación, proyecciones de agua, también deben considerarse. Se usa el principio de desactivación. La protección contra transitorios se instala a través de las bobinas de los contactores. El motor está protegido contra sobrecargas. El cableado y la conexión a tierra cumple con los estándares eléctricos apropiados.

El siguiente paso en el análisis de seguridad es separar los componentes principales del sistema y considerar sus modos de fallo potenciales. En un capítulo anterior examinamos el sistema como tres bloques: ENTRADA, LÓGICA, SALIDA. Al considerar el rendimiento del sistema de seguridad, el cableado también debe incluirse en el análisis.

En los ejemplos de la Categoría B, los componentes son:

- Interruptor de enclavamiento (final de carrera)
- Controlador lógico programable
- Contactor
- Cableado

Interruptor de enclavamiento

El interruptor de final de carrera es un dispositivo mecánico. La tarea que realiza es simple – abrir los contactos cuando la guarda se abre. Muchos años atrás, los interruptores de final de carrera se usaban de esta manera. Pero su diseño tiene desventajas que no permiten un mayor rendimiento de seguridad. Los estándares eléctricos requieren dispositivos de protección contra cortocircuito (por ej., fusibles o interruptores automáticos) para los circuitos derivados. Esta protección puede no ser suficiente para evitar un contacto soldado en el interruptor de final de carrera. Los contactos en el interruptor de final de carrera están diseñados para abrirse por la fuerza de un resorte. Desafortunadamente, la fuerza del resorte no siempre es suficiente para superar la fuerza de un contacto soldado. Una segunda consideración es el resorte mismo. El flexionado repetido puede eventualmente producir la ruptura, y la fuerza ejercida sobre los contactos puede no ser suficiente para abrir el circuito. Otros fallos internos en el cabezal del operador o en el varillaje pueden también hacer que los contactos permanezcan cerrados cuando la guarda se abre. Otra consideración importante es la neutralización. Cuando se abre la guarda, el interruptor de final de carrera se anula fácilmente empujando la actuador a la posición accionada y reteniéndola en su lugar con cinta adhesiva, con un cable u otras herramientas simples.

Controlador lógico programable

Los PLC son el sistema de control preferido para las máquinas. Los dispositivos de entrada, como el interruptor de final de carrera con enclavamiento, se conectan a los módulos de entrada. Los dispositivos de salida, como los contactores, se conectan a los módulos de salida. El dispositivo lógico asigna los dispositivos de entrada a los dispositivos de salida apropiados bajo las condiciones lógicas deseadas.

Si bien la fiabilidad de los PLC ha mejorado significativamente desde su presentación, con el transcurso de tiempo de desgastan y fallan. El diseñador del sistema de seguridad debe entender los mecanismos de fallo potencial y si dicho fallo resultará en una condición peligrosa. Los PLC tienen dos categorías de fallo principales: hardware y software. Los fallos de hardware pueden producirse internamente en los módulos de entrada, lógico o de salida. Estos fallos pueden causar que las salidas permanezcan activadas, incluso si se ha iniciado un comando de paro. Los fallos de software en el programa de aplicación o en el firmware también pueden causar que las salidas permanezcan energizadas incluso cuando se haya iniciado un comando de paro.

Contactor

Los contactores activan los accionamientos de la máquina, los motores, solenoides, calefactores y otros tipos de accionamientos. Los accionamientos utilizan altas corrientes, y algunos tienen corriente de entrada al momento del arranque que puede ser 10 veces su valor de estado estable. Los contactores siempre deben tener sus contactos de alimentación protegidos por dispositivos de protección contra sobrecarga y cortocircuito para evitar la soldadura. Aun con esta protección, existe el potencial de que los contactos de conmutación de alimentación eléctrica permanezcan cerrados. Esto puede deberse a soldadura o atascamiento del inducido. Cuando se produce un fallo de esta naturaleza, el botón de paro queda inoperativo y la máquina deberá desactivarse mediante el desconectador principal. Los contactores deben inspeccionarse con regularidad para detectar si hay conexiones flojas que puedan causar sobrecalentamiento y distorsión. El contactor debe cumplir con los estándares pertinentes que abarcan las características y condiciones de uso requeridas. Los estándares IEC 60947-4-1 y IEC 60947-5-1 describen las pruebas detalladas que deben pasar los contactores para uso en diversas aplicaciones.

Cableado

Si bien el diseño e instalación según el estándar eléctrico apropiado reduce la probabilidad de fallos de cableado, estos pueden ocurrir, y de hecho ocurren. Los fallos de cableado que deben considerarse incluyen los cortocircuitos y los circuitos abiertos. El análisis de cortocircuitos debe incluir cortocircuitos a la alimentación eléctrica, a tierra o a otros circuitos que puede causar una condición peligrosa.

Interruptores de arranque y paro

Es necesario considerar los interruptores de arranque y paro. Si el botón Start entra en fallo por cortocircuito, la máquina volverá a arrancar inesperadamente cuando se suelte el botón Start o se cierre la guarda. Afortunadamente, la guarda debe estar cerrada para que arranque el motor. Si la guarda está cerrada, entonces el acceso a la pieza peligrosa debe protegerse. Un botón Stop roto o un cortocircuito en sus contactos inhibirá la ejecución del comando de paro. Nuevamente, la guarda se cierra de modo que se proteja el acceso a la pieza peligrosa.

Las piezas con fines de seguridad del sistema de control deben hacer interfaz con las piezas no relacionadas a la seguridad. Puesto que los fallos en los dispositivos de control de arranque y paro no deben causar una pérdida de la función de seguridad, estos dispositivos no se consideran parte del sistema de seguridad. Este circuito de arranque/paro/retención simboliza las partes no relacionadas a la seguridad del circuito de control de la máquina y pueden sustituirse con un PLC.

La Categoría B proporciona los cimientos para el diseño de un sistema de seguridad. Si bien un diseño, selección e instalación apropiados proporcionan la base para un sistema robusto, muchos factores individuales potenciales pueden causar la pérdida del sistema de seguridad. Teniendo en cuenta estos factores es posible minimizar las posibilidades de fallo y peligro. El uso de la Categoría B por si sola no es lo apropiado para la mayoría de aplicaciones relacionadas a la seguridad.

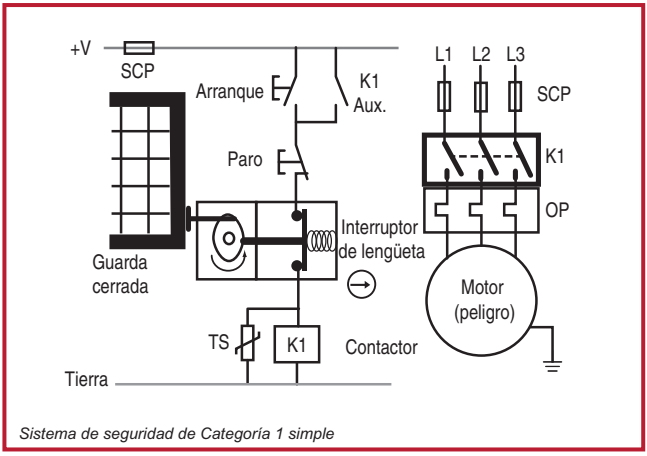
Categoría 1

La Categoría 1 requiere que el sistema cumpla con los términos de la categoría B y el uso de componentes de seguridad debidamente probados. ¿Qué son exactamente los componentes de seguridad y cómo sabemos si han sido debidamente probados? El estándar ISO 13849-2 ayuda a responder esas preguntas para los sistemas mecánicos, hidráulicos neumáticos y eléctricos. El Anexo D describe los componentes eléctricos.

Los componentes se consideran debidamente probados si han sido usados de manera exitosa en muchas aplicaciones similares. Los componentes de seguridad recientemente diseñados se consideran debidamente probados si han sido diseñados y verificados en cumplimiento de los estándares apropiados.

Componente debidamente probado	**Estándar**
Interruptor con accionamiento de modo positivo (acción de apertura directa)	IEC 60947-5-1
Dispositivo de paro de emergencia	ISO 13850, IEC 60947-5-5
Fusible	IEC 60269-1
Interruptor automático	IEC 60947-2
Contactores	IEC 60947-4-1, IEC 60947-5-1
Contactos mecánicamente unidos	IEC 60947-5-1
Contactor auxiliar (por ej., contactor, relé de control, relés con guía positiva)	EN 50205 IEC 60204-1, IEC 60947-5-1
Transformador	IEC 60742
Cable	IEC 60204-1
Dispositivos de enclavamiento	ISO 14119
Termostato	IEC 60947-5-1
Presostato	Requisitos para sistemas neumáticos o hidráulicos + IEC 60947-5-1
Dispositivo o equipo de control y conmutación de protección (CPS)	IEC 60947-6-2
Controlador lógico programable	IEC 61508, IEC 62061

Al aplicar componentes debidamente probados según nuestro sistema de Categoría B, el interruptor de final de carrera sería reemplazado por un interruptor de accionamiento por lengüeta de apertura directa y el contactor sería sobredimensionado para brindar mayor protección contra contactos soldados.



Sistema de seguridad de Categoría 1 simple

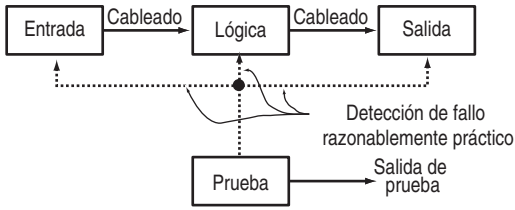
Aquí se muestran los cambios en un sistema de Categoría B simple para lograr la Categoría 1. El dispositivo de enclavamiento y el contactor desempeñan papeles clave en la desconexión de la energía del accionador, cuando se necesita acceso a la pieza peligrosa. El dispositivo con enclavamiento de lengüeta cumple con los requisitos del estándar IEC 60947-5-1 para los contactos de acción de apertura directa, lo cual se muestra mediante el símbolo de flecha dentro del círculo. Con los componentes debidamente probados, la probabilidad de que se desconecte la energía es mayor para la Categoría 1 que para la Categoría B. El uso de componentes debidamente probados está diseñado para evitar una pérdida de la función de seguridad. Incluso con estas mejoras, un fallo individual puede causar la pérdida de la función de seguridad.

Podemos aplicar estos mismos principios al sistema de Categoría B basado en PLC para mejorar el rendimiento de la seguridad a Categoría 1? La respuesta puede ser positiva o negativa. De hecho, reemplazar todos los interruptores de final de carrera que operan en modo negativo con dispositivos de enclavamiento de acción de apertura directa y sobredimensionar los contactores mejorará la probabilidad de que se ejecute la función de seguridad. El PLC entonces se convierte en el centro de la atención. ¿Se ha usado el PLC en muchas aplicaciones similares? ¿Se ha validado y es estable el programa lógico, o requiere afinarse constantemente para hacer mejoras y ajustes? ¿Se ha revisado recientemente el firmware (la parte del software que el usuario no puede modificar)? ¿Cuál es el historial de fallos a peligro en muchas aplicaciones similares? ¿Se han tomado pasos para eliminar o reducir estos fallos a niveles aceptables? En teoría, es posible considerar un PLC como un componente debidamente probado basado en una construcción probada en el uso. Adoptar este método para un dispositivo como un PLC sería una compromiso significativo que implicaría un nivel extremadamente alto de registros y análisis. Para simplificar la situación y evitar el uso arbitrario de PLC “ordinarios”, el estándar ISO 13849-1:1999 indica que “a nivel de componentes electrónicos individuales solamente, normalmente no es posible lograr la Categoría 1”.

Las Categorías B y 1 se basan en la prevención. El diseño está previsto para evitar una situación peligrosa. Cuando la prevención por sí sola no proporciona suficiente reducción del riesgo, deberá usarse la detección de fallos. Las categorías 2, 3 y 4 se basan en la detección de fallos, con requisitos cada vez más exigentes para lograr altos niveles de reducción del riesgo.

Categoría 2

Además cumplir con los requisitos de la Categoría B y usar principios de seguridad debidamente comprobados, el sistema de seguridad debe someterse a pruebas para cumplir con la Categoría 2. Las pruebas deben diseñarse para detectar fallos dentro de las partes relacionadas a la seguridad del sistema de control. Si no se detectan fallos, la máquina podrá funcionar. Si se detectan fallos, la prueba debe iniciar una acción. Siempre que sea posible, la acción debe llevar a la máquina a un estado de seguridad.

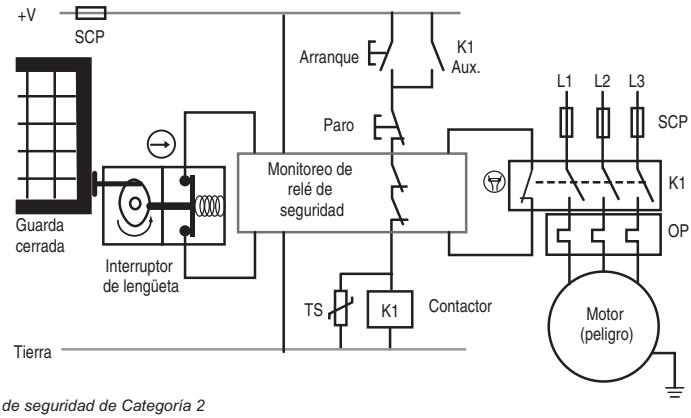


La prueba debe proporcionar una detección de fallos razonablemente práctica. El equipo que realiza la prueba puede ser una parte integral del sistema de seguridad o una pieza separada del equipo.

Las prueba debe ser realizada:

- cuando la máquina se activa inicialmente,
- antes de la iniciación de una pieza de peligro, y
- periódicamente si fue considerado necesario por la evaluación de riesgos

Las palabras “siempre que sea posible” y “razonablemente práctico” indican que no todos los fallos son detectables. Puesto que este es un sistema de un solo canal (es decir, un cable conecta la entrada a la lógica y a la salida), un solo fallo puede causar la pérdida de la función se seguridad. En algunos casos, la Categoría 2 no puede aplicarse completamente a un sistema de seguridad porque no todos los componentes pueden verificarse.

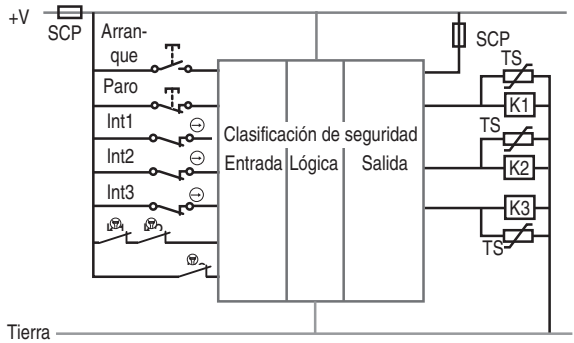


Sistema de seguridad de Categoría 2

Aquí se muestra un sistema de Categoría 1 simple mejorado para cumplir con los requisitos de la Categoría 2. Un relé de control de seguridad (MSR) realiza la prueba. En el momento del encendido el MSR verifica sus componentes internos. Si no se detectan fallos, el MSR verifica el interruptor de lengüeta monitorizando la alternación de sus contactos. Si no se detectan fallos y la guarda está cerrada, entonces el MSR verifica el dispositivo de salida: los contactos mecánicamente unidos del contactor. Si no se detectan fallos y el contactor está desactivado, el MSR activará su salida interna y conectará la bobina de K1 al botón Stop. En este punto, las partes no relacionadas a la seguridad del sistema, el circuito de arranque/paro/enclavamiento, puede activar y desactivar la máquina.

Al abrir la guarda las salidas del MSR se desactivan. Cuando la guarda se vuelve a cerrar, el MSR repite las verificaciones del sistema de seguridad. Si no se detectan fallos, el MSR activa su salida interna. El MSR permite que este circuito cumpla con la Categoría 2 realizando pruebas en el dispositivo de entrada, el dispositivo lógico (en sí mismo) y el dispositivo de salida. La prueba se realiza al momento del arranque inicial y antes de la condición de riesgo.

Con sus capacidades lógicas inherentes, un sistema de seguridad basado en PLC puede diseñarse para cumplir con las especificaciones de la categoría 2. Como se indicó en la descripción de la Categoría 1 anteriormente, se convierte en un reto la justificación debidamente comprobada del PLC (inclusive sus capacidades de prueba). Para sistemas de seguridad complejos que requieren una clasificación de Categoría 2, un PLC con clasificación de seguridad según IEC 61508 debe sustituirse por el PLC no relacionado a la seguridad.



Sistema de seguridad de Categoría 2 compleja

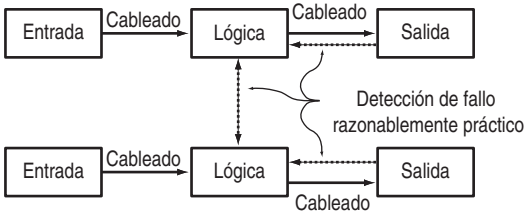
Aquí se muestra un ejemplo de un sistema complejo que usa un PLC de seguridad. Un PLC de seguridad cumple con los requisitos de ser debidamente comprobado según el estándar apropiado y de acuerdo a su diseño. Los contactos mecánicamente unidos de los contactores son alimentados a la entrada del PLC para fines de prueba. Estos contactos pueden estar conectados en serie a un terminal de entrada o a terminales de entrada individuales, dependiendo de la lógica del programa.

Si bien se usan componentes de seguridad debidamente comprobados, un solo fallo que ocurra entre las verificaciones puede causar la pérdida de la función de seguridad. Por lo tanto, se usan sistemas de Categoría 2 en aplicaciones de menor riesgo. Cuando se necesitan niveles más altos de tolerancia a fallos, el sistema de seguridad debe cumplir con las especificaciones de las Categorías 3 ó 4.

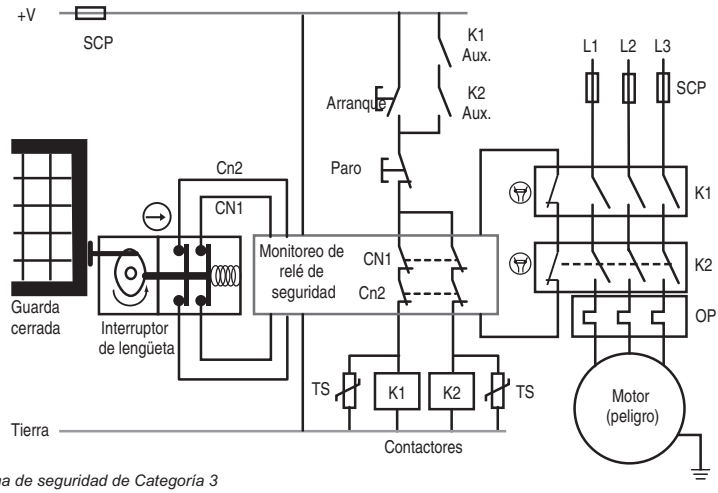
Categoría 3

Además de cumplir con los requisitos de la Categoría B y los principios de seguridad debidamente comprobados, la Categoría 3 requiere un rendimiento satisfactorio de la función de seguridad en presencia de un fallo individual. El fallo debe ser detectado durante o antes de que se imponga la siguiente demanda sobre la función de seguridad, siempre que sea razonablemente práctico.

Aquí nuevamente tenemos la frase “siempre que sea razonablemente práctico”. Esto abarca los fallos que pueden no ser detectados. Siempre y cuando el fallo no detectable no resulte en la pérdida de la función de seguridad, la función de seguridad puede cumplir con las especificaciones de la categoría 3. En consecuencia, una acumulación de fallos no detectados puede causar la pérdida de la función de seguridad.



Aquí se presenta un diagrama de bloques par explicar los principios de un sistema de Categoría 3. La redundancia combinada con monitorización cruzada y monitorización de salidas se usan para asegurar el rendimiento de la función de seguridad.



Sistema de seguridad de Categoría 3

Aquí se muestra un ejemplo de un sistema de Categoría 3. Un conjunto de contactos redundantes se añade al interruptor con enclavamiento de lengüeta. Internamente el relé de control de seguridad (MSR) tiene circuitos redundantes que realizan monitorización cruzada unos a otros. Un conjunto redundante de contactores desconecta la alimentación eléctrica del motor. Los contactores son monitorizados por el MSR a través los de contactos mecánicamente unidos.

Debe considerarse la detección de fallos para cada parte del sistema de seguridad, así como las conexiones (es decir, el sistema). ¿Cuáles son los modos de fallo de un interruptor de lengüeta de dos canales? ¿Cuáles son los modos de fallo del MSR? ¿Cuáles son los modos de fallo de los contactores K1 y K2? ¿Cuáles son los modos de fallo del cableado?

El interruptor con enclavamiento de lengüeta está diseñado con contactos de apertura directa. Por lo tanto, sabemos que la apertura de guarda está diseñada para abrir un contacto soldado. Esto resuelve un modo de fallo. ¿Existen otros modos de fallo?

El interruptor de acción de apertura directa generalmente está diseñado con un retorno de resorte. Si se retira o se rompe el cabezal, los contactos de seguridad regresan al estado cerrado (de seguridad). Muchos interruptores con enclavamiento están diseñados con cabezales extraíbles para aceptar los requisitos de instalación de diversas aplicaciones. El cabezal puede retirarse y girarse entre dos a cuatro posiciones.

Puede producirse un fallo cuando no se aplicó el par de apriete correcto a los tornillos de montaje del cabezal. Con esta condición, la vibración prevista de la máquina puede causar que los tornillos de montaje del cabezal se aflojen. El cabezal de operación, bajo presión del resorte, retira la presión de los contactos de seguridad y los contactos de seguridad se

cierran. Consecuentemente, abrir la guarda no abre los contactos de seguridad y se produce un fallo en la seguridad.

De manera similar, el mecanismo de operación al interior del interruptor debe revisarse. ¿Cuál es la probabilidad de que un fallo de un solo componente cause la pérdida de la función de seguridad? Estas preguntas se responderán en un futuro próximo a medida que deban proporcionarse el tiempo medio para fallo peligroso, la cobertura de diagnósticos y la fracción de fallos no peligrosos para satisfacer el requisito de conocimientos cada vez mayor requeridos para asegurar el rendimiento de la función de seguridad.

Una práctica común es usar dispositivos con enclavamiento de lengüeta con contactos dobles en circuitos de Categoría 3. Este uso debe basarse en excluir el fallo individual del interruptor para abrir los contactos de seguridad. Esto se considera “exclusión de fallo” y se describe posteriormente en este capítulo.

Un relé de control de seguridad electromecánico (MSR) es un dispositivo de baja complejidad que a menudo es evaluado por terceros y se le asigna un nivel de categoría. El MSR generalmente incluye capacidad de doble canal, monitorización de canal cruzado, monitorización de dispositivos externos y protección contra cortocircuito. No se han escrito estándares específicos para proporcionar orientación sobre el diseño o uso de relés de control de seguridad. Los MSR son evaluados por su capacidad de realizar la función de seguridad según ISO 13849-1 o su predecesor EN 954-1. Para satisfacer los requisitos una clasificación de categoría de seguridad del sistema, el MSR debe ser de la misma clasificación o de una más alta.

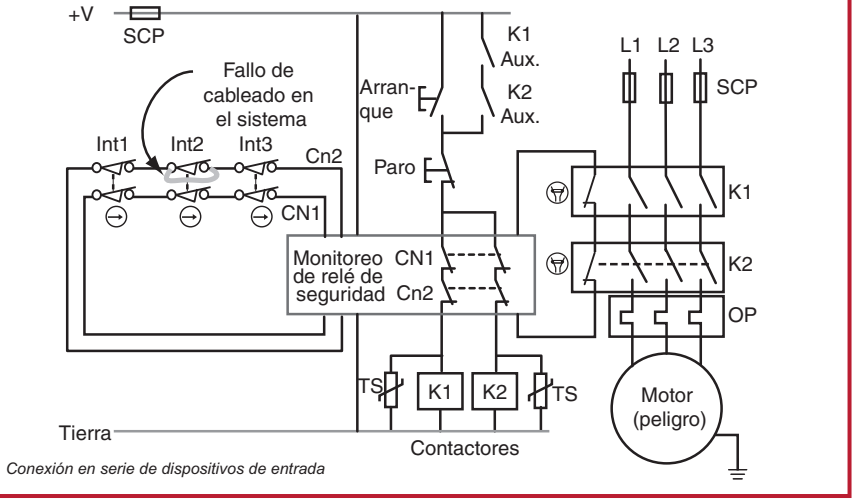
Dos contactores ayudan a asegurar que la función de seguridad sea satisfecha por los dispositivos de salida. Con protección contra sobrecarga y cortocircuito, la probabilidad de que falle el contactor con contactos soldados es pequeña pero no imposible. Un contactor también puede fallar debido a los contactos de conmutación de alimentación eléctrica cerrados por una bobina soldada. Si un contactor falla, el segundo contactor desconectará la alimentación eléctrica de la pieza peligrosa. El MSR detectará el contactor en fallo el siguiente ciclo de la máquina. Cuando se cierra la compuerta y se presiona el botón Start, los contactos mecánicamente unidos del contactor permanecerán abiertos y el rearme no podrá cerrar sus contactos de seguridad revelando de ese modo el fallo.

Fallos no detectados

Como se indicó anteriormente, algunos fallos no pueden detectarse. Estos fallos, por sí mismos, no causan la pérdida de la función de seguridad. Al evaluar los fallos es necesario hacer una serie de preguntas. La respuesta a la primera pregunta conducirá a diferentes preguntas de seguimiento: *Primera pregunta:* ¿Puede detectarse el fallo?

Si la respuesta es sí, entonces necesitamos conocer si esta detección es inmediata o en la siguiente demanda. También necesitamos conocer si puede ser enmascarado (es decir, restablecido) por otros dispositivos.

Si la respuesta es no, ¿causó el fallo la pérdida de la función de seguridad? ¿Causaría un fallo subsiguiente la pérdida de la función de seguridad?

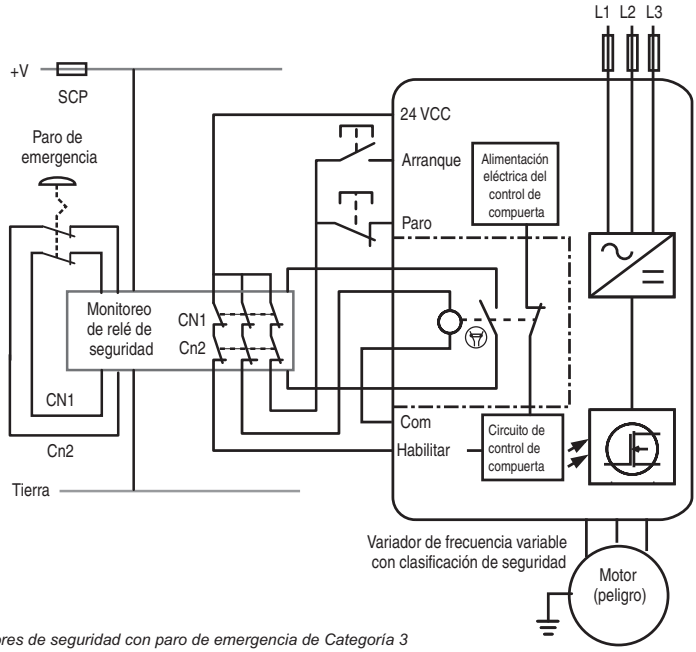


Conexión en serie de dispositivos de entrada

Aquí se muestra un método ampliamente usado para conectar múltiples dispositivos a un relé de control de seguridad. Cada dispositivo dispone de dos contactos de acción de apertura directa normalmente cerrados. Estos dispositivos pueden ser una combinación de dispositivos de enclavamiento o botones de paro de emergencia. Este método ahorra costes de cableado ya que los dispositivos de entrada están conectados en cadena. Suponga que se produce un fallo por cortocircuito en uno de los contactos. ¿Puede detectarse este fallo?

Cuando los interruptores Sw1 y Sw3 se abren, el MSR desconecta la alimentación eléctrica correctamente del accionador. Cuando Sw1 y Sw2 se cierran, el accionador puede volverse a arrancar presionando el botón Start. Durante estas acciones el fallo no se detectó, pero no condujo a la pérdida de la función de seguridad. ¿Qué sucede cuando Sw2 se abre?

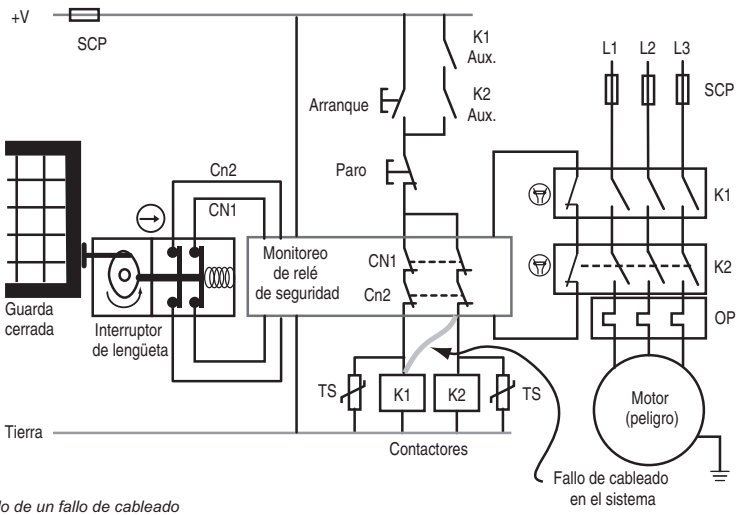
Cuando Sw2 se abre, Ch1 se abre y Ch2 permanece cerrado. El MSR desactiva el motor porque Ch1 se abrió. Cuando Sw2 se cierra el motor no puede arrancar cuando el botón Start está presionado, porque Ch2 no se abrió. El fallo es detectado. La debilidad de este rearme es que el interruptor Sw1 ó Sw3 pueden abrirse y cerrarse y enmascarar el fallo. Un fallo subsiguiente (un cortocircuito en el segundo contacto o Sw2) causará la pérdida de la función de seguridad. La conexión en serie de los contactos mecánicos está limitada a la categoría 3 ya que puede causar la pérdida de la función de seguridad debido a una acumulación de los fallos.



Variadores de seguridad con paro de emergencia de Categoría 3

Aquí se muestra un circuito de categoría 3 que usa un variador de frecuencia con clasificación de seguridad. Recientes avances en la tecnología de variador junto con la actualización de los estándares eléctricos permiten que los variadores con clasificación de seguridad se usen en circuitos de paro de emergencia sin necesidad de un contactor doble de seguridad.

Presionar el paro de emergencia abre las salidas del MSR. Esto envía una señal de paro al variador, retira la señal de habilitación y abre la alimentación de control de la compuerta. El variador ejecuta un paro de Categoría 0 – desconexión inmediata de la alimentación eléctrica al motor. El variador logra la categoría 3 porque dispone de señales redundantes para desconectar la alimentación eléctrica del motor: la habilitación un relé con guía positiva. El relé con guía positiva proporciona realimentación al variador. El mismo variador es analizado para determinar que un fallo no cause la pérdida de la función de seguridad.

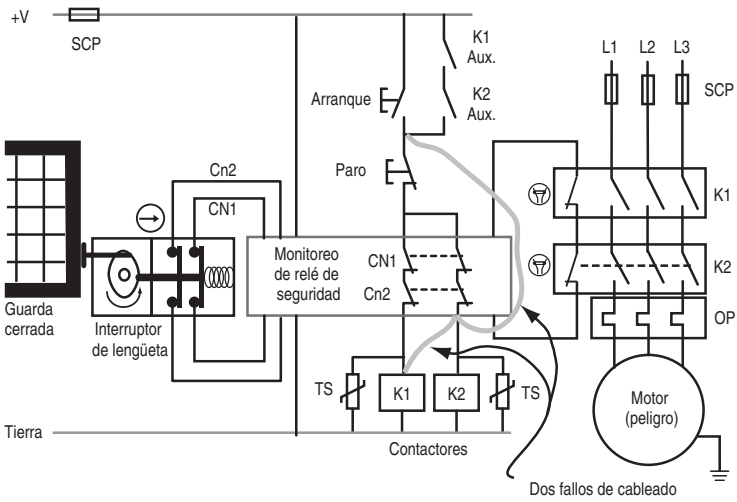


Ejemplo de un fallo de cableado

Aquí se muestra un ejemplo de un fallo de cableado, un cortocircuito, desde la salida de seguridad del canal 2 del MSR hasta la bobina del contactor K1. Todos los componentes están operando correctamente. Este fallo de cableado puede ocurrir antes de la puesta en marcha de la máquina en una fecha posterior durante el mantenimiento o durante las mejoras.

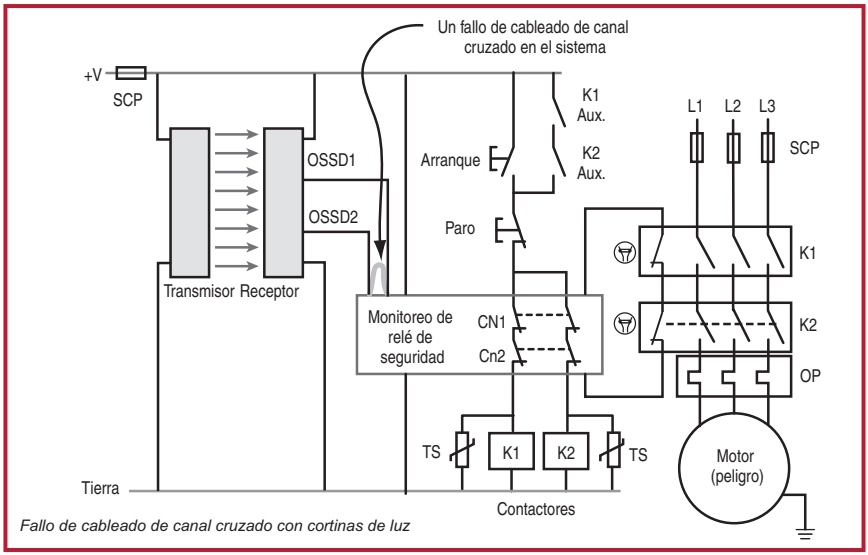
¿Puede detectarse este fallo?

Este fallo no puede ser detectado por el sistema de seguridad como se muestra. Afortunadamente, no causa la pérdida de la función de seguridad. Este fallo, así como el fallo de Ch1 a K2, debe ser detectado durante la puesta en marcha.



Dos fallos causan la pérdida de la función de seguridad

Aquí se muestra un segundo fallo que causa la pérdida de la función de seguridad. Este es un cortocircuito de la salida del MSR al botón de rearme. Al momento del encendido con la guarda cerrada, estos dos fallo no se detectan. El presionar el botón de rearme inicia el riesgo. El abrir la guarda no causa que se elimine el riesgo.



Fallo de cableado de canal cruzado con cortinas de luz

Aquí se muestra un ejemplo de sistema de seguridad con las barreras de seguridad (saldas OSSD)

¿Puede detectar este fallo el sistema de seguridad?

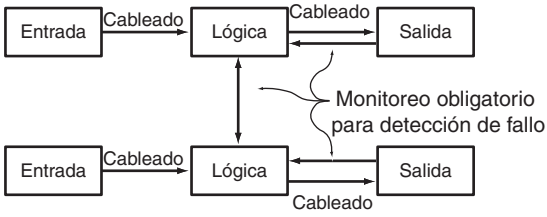
El MSR no puede detectar este fallo porque ambas entradas están cableadas al positivo. En este ejemplo el fallo de cableado es detectado por la cortina de luz. Algunas cortinas de luz usan una técnica de detección de fallo llamada prueba de impulso. Con estas barreras de seguridad la detección del fallo es inmediata y la cortina de luz desactiva su salida. En otros, la detección se realiza cuando la barrera de seguridad se restablece. Cuando la barrera de seguridad intenta activar su salida, se detecta el fallo y la salida permanece desactivada. En cualquiera de los casos, la riesgo permanece inactivo en presencia del fallo.

Detección de fallo por prueba de impulso

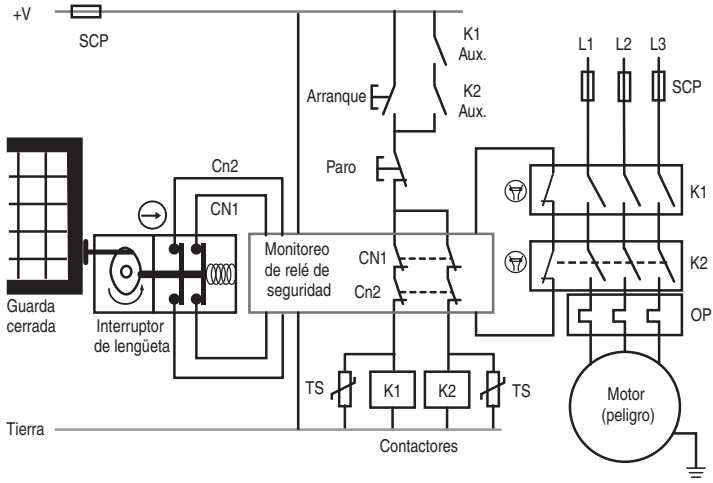
Los circuitos están diseñados para portar corriente cuando el sistema de seguridad está activo y la pieza peligrosa está protegida. La prueba de pulsos es una técnica en la que la corriente del circuito cae a cero por un período muy corto. La duración es demasiado corta para que el circuito de seguridad responda y desactive el accionamiento, pero es suficientemente largo para que un sistema basado en microprocesador lo detecte. Los impulsos en los canales están desplazados uno con respecto a otro. Si ocurre un cortocircuito de fallo cruzado, el microprocesador detecta los impulsos en ambos canales e inicia un comando para desactivar el accionamiento.

Categoría 4

Al igual que la Categoría 3, la Categoría 4 requiere que el sistema de seguridad cumpla con las especificaciones de la Categoría B, use principios de seguridad y realice la función de seguridad en presencia de un fallo individual. A diferencia de la Categoría 3 donde una acumulación de fallos puede causar la pérdida de la función de seguridad, la Categoría 4 requiere el rendimiento de la función de seguridad en presencia de una acumulación de fallos. Al considerar una acumulación de fallos, 2 fallos podrían ser suficientes, aunque 3 fallos pueden ser necesarios para algunos diseños.



Aquí se muestra el diagrama de bloques para la Categoría 4. La monitorización de ambos dispositivos de salida y la monitorización cruzada es esencial, no sólo cuando es razonablemente práctico. Esto ayuda a diferenciar la Categoría 4 de la Categoría 3.

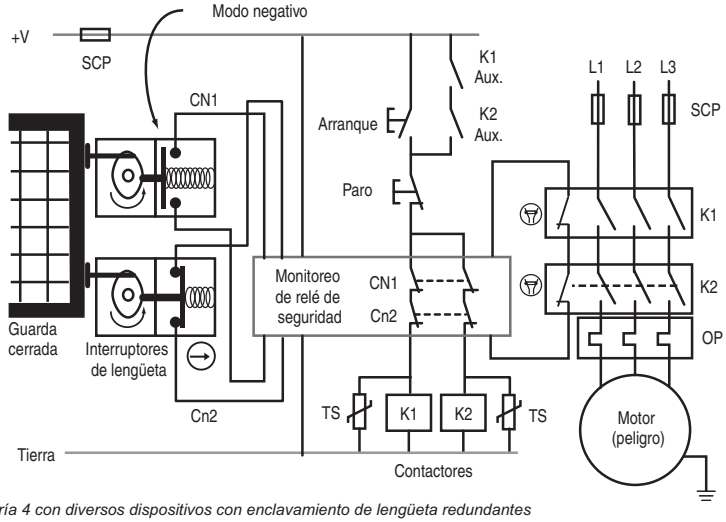


Categoría 4 con exclusión de fallo en el dispositivo con enclavamiento de lengüeta

Aquí se muestra un ejemplo de circuito de Categoría 4 que usa exclusión de fallo en el dispositivo con enclavamiento de lengüeta. La exclusión del fallo elimina la consideración de fallo de apertura de los contactos del dispositivo de enclavamiento con lengüeta. La exclusión del fallo debe ser justificada y documentada técnicamente. En la justificación deben considerarse la velocidad del accionador, el alineamiento del accionador, los paros mecánicos y un cabezal operativo protegido.

Si el diseñador del sistema de seguridad prefiere usar dispositivos de enclavamiento de tipo lengüeta pero no está seguro del uso de la exclusión de fallo en los dispositivos de enclavamiento, entonces pueden usarse dos dispositivos con enclavamiento de lengüeta para cumplir con los requisitos de la Categoría 4. El relé de control de seguridad debe tener clasificación de Categoría 4 y los contactores de salida, con contactos mecánicamente unidos, deben monitorizarse.

La diversidad puede aplicarse para reducir más aún la probabilidad de pérdida de la función de seguridad debido al modo común o fallos de causa común, uno de los interruptores con enclavamiento de lengüeta puede convertirse al modo negativo. Un interruptor que funciona en modo negativo es aceptable siempre que un segundo interruptor use contactos de acción de apertura directa. El siguiente diagrama muestra un ejemplo de esta estrategia diversa. Con esta estrategia, el MSR debe diseñarse para aceptar entradas normalmente abiertas y normalmente cerradas.



Categoría 4 con diversos dispositivos con enclavamiento de lengüeta redundantes

Clasificaciones de los componentes y del sistema

El estándar ISO 13849-1 requiere clasificaciones de componentes así como clasificaciones del sistema. Esto genera alguna confusión que puede aclararse con el entendimiento de los componentes y sus capacidades. Lo que hallamos es que un componente con clasificación de categoría 1 puede usarse en un sistema con clasificación de categoría 2, 3 ó 4, según la arquitectura del sistema.

La descripción de las categorías B y 1 indica que se basan en la prevención, mientras que las descripción de las categorías 2, 3 y 4 indica que se basan en la detección. Estas categorías se aplican según los componentes y también según el sistema. Un sistema de seguridad típico consta de un interruptor con enclavamiento de seguridad, un relé de seguridad y un contactor de seguridad. El dispositivo de enclavamiento y el contactor son dispositivos con Categoría 1 porque sólo se basan en la prevención. Utilizan principios de seguridad pero no realizan ninguna detección ni autoverificación. Estos dispositivos pueden usarse en redundancia en sistemas de Categoría 3 y 4, siempre que el dispositivo lógico realice la detección.

Los dispositivos lógicos no sólo se basan en la prevención sino también en la detección. Se verifican internamente par asegurar el desempeño correcto. Por lo tanto, los relés de control de seguridad y los controladores de seguridad programables tienen clasificaciones de Categoría 2, 3 ó 4.

Consideraciones y exclusiones de fallo

El análisis de seguridad requiere un análisis extenso de los fallos y un entendimiento minucioso del rendimiento del sistema de seguridad en la presencia de fallos. Los estándares ISO 13849-1 y ISO 13849-2 proporcionan detalles sobre las consideraciones de fallos y las exclusiones de fallos.

Si un fallo provoca otro fallo en la instalación, éste y los fallos subsiguientes se considerarán un solo fallo.

Si dos o más fallos se producen como resultado de una misma causa, los fallos se considerarán como un solo fallo. Esto se conoce como fallo por causas comunes.

La presencia de dos o más fallos simultáneamente se considera altamente improbable y no se considera en este análisis. Entre las demandas impuestas sobre el sistema de seguridad, la suposición básica es que sólo se produce un fallo.

Cuando los componentes y los sistemas se diseñan según los estándares apropiados, la presencia del fallo puede excluirse. Por ejemplo, el fallo de apertura de los contactos normalmente cerrados puede excluirse si el interruptor está construido según el estándar IEC 60947-5-1 Anexo K. El estándar ISO 13849-2 proporciona una lista de exclusiones de fallos.

Sistemas que realizan paros de Categoría 1

Todos los ejemplos anteriores mostraron paros de Categoría 0 (desconexión inmediata de la alimentación eléctrica de los accionadores). Un paro de Categoría 1 (aplicar el freno hasta lograr el detenerse y luego desconectar la alimentación eléctrica del accionador) se logra mediante una salida con retardo de tiempo. Una guarda enclavada con bloqueo de guarda generalmente es parte de un sistema de paro de Categoría 1. Esto mantiene la guarda bloqueada en posición cerrada hasta que la máquina llegue a un estado de seguridad (por ejemplo, parado).

Parar una máquina sin considerar adecuadamente el controlador programable puede afectar el reinicio y podría causar graves daños a la misma. Un PLC estándar (no relacionado a la seguridad) en solitario no puede usarse en una tarea de paro de seguridad; por lo tanto deberán considerarse otras estrategias.

A continuación se ofrecen tres soluciones posibles:

1. PLC de seguridad

Uso de un PLC que integre unalto nivel de funcionalidades en seguridad. En la práctica, esto se lograría usando un PLC de seguridad, tal como un GuardLogix, para control con y sin fines de seguridad.

2. Relé de seguridad con salidas retardadas

Se usa un relé de seguridad con salidas inmediatas y retardadas (por ej. e MSR138DP). La salidas de acción inmediata se conectan a las entradas en el dispositivo programable (por ej., P.L.C.) y las salidas de acción retardada se conectan al contactor. Cuando el interruptor de enclavamiento de guarda se activa, conmutan las salidas inmediatas en el interruptor de relé de seguridad. Estas indican al sistema programable que realice un paro con la secuencia correcta. Después que transcurre el tiempo suficiente para permitir este proceso, la salida retardada conmuta y aísla el contactor principal.

Nota: Cualquier cálculo para determinar el tiempo total de paro debe tener en cuenta el período de retardo de la salida del relé de seguridad. Esto es especialmente importante cuando se usa este factor para determinar la posición de los dispositivos según el cálculo de la distancia de seguridad.

3. Dispositivos con bloqueo de guarda controlados por el sistema programable

Esta solución proporciona el alto nivel de integridad del cableado combinado con la capacidad de proporcionar una desactivación en la secuencia correcta, pero sólo es aplicable donde la fuente de peligro está protegida por una guarda.

Para permitir la abertura de la puerta de la guarda, el bloqueo del bobina del interruptor de enclavamiento debe recibir una señal de desbloqueo del P.L.C. Esta señal sólo se dará después que se haya completado una secuencia de comando de paro, para reducir el

riesgo de daño a la herramienta o pérdida del programa. Cuando se activa la bobina, la puerta puede abrirse, lo cual causa que los contactos del circuito de control del interruptor de enclavamiento aíslen el contactor de la máquina. A fin de evitar señales de liberación falsas o de descarga de la máquina, quizás sea necesario usar una unidad con retardo de tiempo (por ej., MSR178DP) o un detector de velocidad cero (por ej. CU2) junto con el P.L.C.

Requisitos del sistema de control de seguridad en los EE.UU.

Los requisitos de un sistema de control con fines de seguridad en los EE.UU. pueden encontrarse en una serie de estándares diferentes, pero se destacan dos documentos: ANSI B11.TR3 y ANSI R15.06. El informe técnico ANSI B11.TR3 establece cuatro niveles caracterizados por la cantidad prevista de reducción de riesgo que cada uno puede proporcionar:

Los requisitos para cada nivel se indican a continuación.

Grado más bajo

De conformidad con ANSI B11.TR3, las medidas de protección que proporcionan el grado más bajo de reducción de riesgos incluyen sistemas de control eléctrico, electrónico, hidráulico o neumático y controles asociados usando una configuración de un solo canal. Está implícito el requisito de usar dispositivos con clasificación de seguridad. Esto concuerda estrictamente con la Categoría 1 del estándar ISO 13849-1.

Reducción de riesgo baja/intermedia

Las medidas de protección que proporcionan reducción de riesgos baja/intermedia según ANSI B11.TR3 incluyen sistemas de control que tienen redundancia que puede comprobarse manualmente para verificar el rendimiento del sistema de seguridad. Al examinar exclusivamente los requisitos, el sistema emplea redundancia simple. No se requiere la función de verificación. Sin verificación, uno de los componentes de seguridad redundante puede fallar y el sistema de seguridad no lo notará. Esto resultaría en un sistema de un solo canal. Este nivel de reducción de riesgos concuerda mejor con la Categoría 2 cuando se usa verificación.

Reducción de riesgo alta/intermedia

Las medidas de protección que proporcionan reducción de riesgos alta/intermedia según ANSI B11.TR3 incluyen sistemas de control que tienen redundancia con autoverificación al momento de la puesta en marcha para confirmar el rendimiento del sistema de seguridad. Para las máquinas que arrancan cada día, la autoverificación proporciona una mejora significativa en la integridad de la seguridad con respecto al sistema puramente redundante. Para las máquinas que funcionan 24 horas al día, 7 días a la semana, ésta es una mejora marginal. El empleo de monitorización periódica del sistema concuerda con los requisitos de la Categoría 3.

El más alto grado de reducción de riesgo

ANSI B11.TR3 proporciona la más alta reducción de riesgos mediante sistemas de control que tienen redundancia con autoverificación continua. La autoverificación debe verificar el rendimiento del sistema de seguridad. El reto para el diseñador del sistema de seguridad es determinar lo que es continuo. Muchos sistemas de seguridad realizan sus verificaciones al momento de la puesta en marcha y cuando se impone una demanda sobre el sistema de seguridad.

Por el contrario, algunos componentes realizan autoverificación continua. Las barreras de seguridad, por ejemplo, activan y desactivan sus indicadores LED secuencialmente. Si se produce un fallo, la barrera de seguridad desactiva todas sus salidas antes de que se imponga una demanda sobre el sistema de seguridad, a medida que se autoverifica continuamente. Los relés basados en microprocesador y los PLC de seguridad son otros componentes que realizan autoverificación continua.

El requisito del sistema de control de autoverificación “continua” no tiene el propósito de limitar la selección de componentes a las barrera de seguridad y unidades lógicas basadas en microprocesador. La verificación debe realizarse al momento de la puesta en marcha y después de cada demanda impuesta sobre el sistema. Este nivel de reducción de riesgos tiene el propósito de concordar con la Categoría 4 del estándar ISO 13849-1.

Estándares para robots: EE.UU. y Canadá

Los estándares para robots en los EE.UU. (ANSI RIA R15.06) y en Canadá (CSA Z434-03) son similares. Ambos tienen cuatro niveles similares a las categorías de EN 954-1:1996.

Simple

En su nivel más bajo, los sistemas de control de seguridad simples deben diseñarse y construirse con circuitos de un solo canal aceptados, y estos sistemas puede ser programables. En Canadá, este nivel está más restringido para fines de señalización y avisos. El reto para el diseñador del sistema de seguridad es determinar lo que es “aceptado”. ¿Qué es un circuito de un solo canal aceptado? ¿Para quién es aceptable el sistema? La categoría Simple concuerda más estrictamente con la Categoría B de EN 954-1:1996.

Un canal

El siguiente nivel es un sistema de control de seguridad de un solo canal que

- se basa en hardware o es un dispositivo de software/firmware con fines de seguridad
- incluye componentes de seguridad; y
- se usa de acuerdo con las recomendaciones de los fabricantes y
- usa diseños de circuitos probados.

Un ejemplo de un diseño de circuito probado es un dispositivo de interrupción positivo electromecánico de un solo canal que transmite una señal de paro en estado desenergizado. Puesto que es un sistema de un solo canal, el fallo de un solo componente puede conducir a la pérdida de la función de seguridad. La categoría Simple concuerda más estrictamente con la Categoría 1 de EN 954-1:1996.

Dispositivo de software/firmware con clasificación de seguridad

Si bien los sistemas basados en hardware han sido el método preferido de proporcionar protección de robots, los dispositivos de software/firmware se están convirtiendo en la opción popular por su capacidad de manejar sistemas complejos. Se permite el uso de dispositivos de software/firmware (PLC de seguridad o controladores de seguridad) siempre y cuando tengan clasificación de seguridad. Esta clasificación requiere que un solo componente con fines de seguridad o un fallo de firmware no cause la pérdida de la función de seguridad. Cuando se detecta un fallo, se detiene la operación automática subsiguiente del robot hasta que se restablezca el fallo.

Para lograr una clasificación de seguridad, el dispositivo de software/firmware debe probarse según un estándar aprobado por una entidad reconocida. En los EE.UU., OSHA mantiene una lista de laboratorios de prueba con reconocimiento nacional (NRTL). En Canadá, el Standards Council of Canada (SCC) mantiene una lista similar.

Un solo canal con monitorización

Los sistemas de control de seguridad de un solo canal con monitorización deben cumplir con los requisitos para un solo canal, tener clasificación de seguridad y utilizar verificación. La verificación de la(s) función(es) de seguridad debe realizarse durante la puesta en marcha de la máquina, y periódicamente durante la operación. Se prefiere la verificación automática sobre la verificación manual.

La operación de verificación permite la operación si no se han detectado fallos, o genera una señal de paro si se detectó un fallo. Deberá proporcionarse una advertencia si un accionamiento permanece activado después que se detuvo el movimiento. Por supuesto, la verificación en sí no debe causar una situación peligrosa. Después de detectar el fallo, el robot debe permanecer en un estado de seguridad hasta que se corrija el fallo.

La categoría de un solo canal con monitorización concuerda más estrictamente con la Categoría 2 de EN 954-1:1996.

Control fiable

El más alto nivel de reducción de riesgos establecido en los estándares para robots de los EE.UU. y Canadá se logra mediante sistemas de control de seguridad que cumplen con los requisitos de control fiable. Los sistemas de control relacionados a la seguridad con control fiable son arquitecturas de dos canales con monitorización. La función de paro del robot no debe evitarse mediante el fallo de un componente individual, inclusive la función de monitorización.

La función de monitorización generará un comando de paro al detectarse un fallo. Si un peligro permanece después que se detiene el movimiento, deberá proporcionarse una señal de advertencia. El sistema de seguridad debe permanecer en un estado de seguridad hasta que se corrija el fallo.

Preferiblemente, el fallo se debe detectar al momento de producirse. Si esto no puede realizarse, entonces el fallo debe detectarse durante el siguiente ciclo del sistema de seguridad.

Los fallos del modo común deben tomase en cuenta si existe una probabilidad significativa de que dicho tipo de fallo ocurra.

Los requisitos canadienses difieren de los requisitos de los EE.UU. por dos requisitos adicionales. Primero, los sistemas de control con fines de seguridad serán independientes de los sistemas de control de programa normales. Segundo, el sistema de seguridad no deberá neutralizarse u omitirse sin detección.

Los sistemas fiables de control concuerdan con las Categorías 3 y 4 de EN 954-1:1996.

Comentarios sobre el control fiable:

El aspecto más fundamental del control fiable es la tolerancia a un solo fallo. Los requisitos establecen cómo el sistema de seguridad debe responder en presencia de “un solo fallo”, “cualquier fallo individual”, o “un fallo de cualquier componente individual”.

Hay tres conceptos muy importantes que deben considerarse respecto a los fallos: (1) no todos los fallos se detectan, (2) añadir la palabra “componente” presenta preguntas acerca del cableado, y (3) el cableado es parte integral del sistema de seguridad. Los fallos del cableado pueden resultar en la pérdida de una función de seguridad.

El propósito de la fiabilidad del control claramente es el rendimiento de la función de seguridad en presencia de un fallo. Si se detectó el fallo, entonces el sistema de seguridad debe ejecutar una acción de seguridad, proporcionar notificación sobre el fallo y detener la operación de la máquina hasta que el fallo sea corregido. Si no se detecta el fallo, entonces la función de seguridad debe realizarse a demanda.

Introducción a la seguridad funcional de los sistemas de control

Importante: *Los estándares y requisitos considerados en esta sección son relativamente nuevos. Todavía se sigue trabajando en algunos aspectos, especialmente respecto a aclaración y combinación de algunos de estos estándares. Por lo tanto, es probable que hayan cambios sobre algunos de los detalles proporcionados. Para obtener la información más reciente, consulte: http://www.ab.com/safety.*

Al momento de la publicación de este documento existe un conocimiento cada vez mayor de las implicaciones de una nueva generación de estándares que abarca la seguridad funcional de los sistemas y dispositivos de control relacionados a la seguridad.

¿Qué es la seguridad funcional?

La seguridad funcional es la parte de la seguridad global que depende del funcionamiento correcto del proceso o equipo en respuesta a sus entradas. El sitio web de la IEC proporciona el siguiente ejemplo para ayudar a aclarar el significado de la seguridad funcional. “Por ejemplo, un dispositivo de protección contra sobretemperatura que utiliza un sensor térmico en los bobinados de un motor eléctrico para desactivar el motor antes de que pueda calentarse en exceso, es un ejemplo de seguridad funcional. Pero proporcionar aislamiento especial para resistir altas temperaturas no es un ejemplo de seguridad funcional (aunque es un ejemplo de seguridad y podría proteger precisamente contra el mismo peligro)”. Como otro ejemplo, comparemos una protección basada en hardware con una guarda con enclavamiento. La guarda basada en hardware no se considera “seguridad funcional” aunque puede proteger contra el acceso a la misma pieza peligrosa que una puerta con enclavamiento. La puerta con enclavamiento es un ejemplo de seguridad funcional. Si se abre la guarda, el enclavamiento actúa como “entrada” para un sistema que alcanza un estado de seguridad. De manera similar, se utiliza equipo de protección personal (PPE) como medida protectora para ayudar a aumentar la seguridad del personal. El equipo de protección personal no se considera seguridad funcional.

La seguridad funcional es un término introducido en el estándar IEC 61508:1998. Desde entonces el término se ha asociado algunas veces con los sistemas de seguridad programables. Esto es un concepto erróneo. La seguridad funcional cubre una amplia gama de dispositivos usados para crear sistemas de seguridad. Dispositivos tales como enclavamientos, barreras de seguridad, relés de seguridad, PLC de seguridad, contactores de seguridad y variadores de seguridad se interconectan para formar un sistema de seguridad, el cual realiza una función específica con fines de seguridad. Esto es seguridad funcional. Por lo tanto, la seguridad funcional de un sistema de control eléctrico es muy importante para el control de peligros que surgen de las piezas en movimiento de la maquinaria.

Se necesita dos tipos de requisitos par lograr la seguridad funcional:

- la función de seguridad y
- la integridad de la seguridad.

El proceso de evaluación de riesgos desempeña un papel clave en el desarrollo de los requisitos de la seguridad funcional. El análisis de riesgos indica los requisitos de la función de seguridad (lo que realiza la función). La evaluación de riesgos proporciona los requisitos de integridad de la seguridad (la probabilidad de que una función de seguridad se realice satisfactoriamente).

Tres estándares de seguridad funcional importantes para sistema de control para maquinaria son:

1. **IEC/EN 61508** "Seguridad funcional de sistemas de control eléctricos, electrónicos y electrónicos programables relacionados con la seguridad"

   Este estándar contiene los requisitos y disposiciones aplicables al diseño de sistemas y subsistemas de electrónica complejos y programables. El estándar es genérico, por lo tanto no está restringido al sector de máquinas.

2. **IEC/EN 62061** "Seguridad de máquinas – Seguridad funcional de sistemas de control relacionados con la seguridad eléctricos, electrónicos y electrónicos programables"

   Es la implementación específica para maquinarias de IEC/EN 61508. Proporciona requisitos aplicables al diseño de nivel del sistema de todos los tipos de seguridad de maquinaria relacionada con sistemas de control eléctricos y también al diseño de subsistemas o dispositivos no complejos. Requiere que los subsistemas programables o complejos satisfagan los requisitos del estándar IEC/EN 61508

3. **EN ISO 13849-1:2008** "Seguridad de máquinas – Piezas relacionadas a la seguridad de los sistemas de control"

   Tiene el propósito de proporcionar una ruta de transición funcional con respecto a las categorías.

Los estándares de seguridad funcional representan un paso importante más allá de los requisitos existentes conocidos, tales como control fiable y los sistemas de categorías de ISO 13849-1:1999 (EN 954-1:1996). Las categorías todavía no están desapareciendo, el estándar original permanecerá vigente hasta 2010 para proporcionar un período de transición a su nueva versión revisada. Esta nueva versión de ISO/EN 13849-1 utiliza el concepto de seguridad funcional y ha introducido nueva terminología y requisitos. En esta sección nos referiremos a la nueva versión como EN ISO 13849-1:2008.

El interés en los nuevos estándares de seguridad funcional aumentará porque representan el futuro y facilitan una mayor flexibilidad y el uso de nueva tecnología para la seguridad de las máquinas.

IEC/EN 62061 e EN ISO 13849-1:2008

Tanto IEC/EN 62061 como EN ISO 13849-1:2008 abarcan sistemas de control eléctricos relacionados con la seguridad. El objetivo es que eventualmente se combinen como dos partes de un estándar con terminología común. Ambos estándares producen los mismos resultados pero emplean métodos diferentes. Su propósito es proporcionar a los usuarios una opción para seleccionar el más idóneo para su situación. Un usuario puede decidir usar cualquiera de los estándares.

Las salidas de ambos estándares son niveles comparables de rendimiento de seguridad o integridad. Las metodologías de cada estándar tienen diferencias apropiadas para usuarios específicos. Una restricción para EN ISO 13849-1:2008 se proporciona en la Tabla 1 de su introducción. Cuando se utiliza tecnología compleja y programable, el máximo PL que debe considerarse es PLd.

La metodología descrita en IEC/EN 62061 tiene el propósito de permitir funcionalidad de seguridad compleja que puede ser implementada por arquitecturas de sistemas que antes eran no convencionales. Esta metodología de EN ISO 13849-1:2008 está diseñada para proporcionar una ruta más directa y menos complicada para una funcionalidad de seguridad convencional implementada por arquitecturas de sistema convencionales.

Una distinción importante entre estos dos estándares es la aplicabilidad a varias tecnologías. La normativa IEC/EN 62061 está limitada a sistemas eléctricos. EN ISO 13849-1:2008 puede aplicarse a sistemas neumáticos, hidráulicos y mecánicos, así como a sistemas eléctricos.

Las siguientes descripciones generales revelan las similaridades subyacentes en valores y razones entre los estándares. Debe entenderse que únicamente son descripciones generales breves. Ambos estándares abarcan mucho más de lo que se muestra aquí y es importante considerar el texto completo de ambos estándares.

La siguiente tabla proporciona un diagrama de flujo simplificado para ayudar al diseñador del sistema de seguridad a determinar cuál de estos dos estándares usar. Cada ruta comparte procesos comunes: funciones de seguridad y evaluación de riesgos. La información de diseño del sistema (por ej., PFH, MTTF, DC, SFF) es diferente puesto que la ruta tiene divergencias de un estándar al otro.

SIL e IEC/EN 62061

IEC/EN 62061 describe tanto la cantidad de riesgo que se reducirá como la capacidad de un sistema de control de reducir dicho riesgo en términos de SIL (nivel de integridad de seguridad). Se usan tres niveles SIL en el sector de maquinarias; SIL1 es el más bajo y SIL3 es el más alto.

Pueden existir riesgos de mayor magnitud en otros sectores tales como la industria de procesos, y por tal razón IEC 61508 y el estándar específico para el sector de procesos, IEC 61511, incluyen SIL4. Un nivel SIL se aplica a una función de seguridad. Los subsistemas

que conforman el sistema que implementa la función de seguridad deben tener una capacidad SIL apropiada. Esto algunas veces se conoce como límite de declaración de SIL (SIL CL). Se requiere un estudio completo y detallado de IEC/EN 62061 para poder aplicarlo correctamente. Algunos de los requisitos de este estándar aplicables más comúnmente se describen de la siguiente manera:

PL y EN ISO 13849-1:2008

EN ISO 13849-1:2008 no utilizará el término SIL; en lugar de ello utiliza el término PL (nivel de rendimiento). En muchos aspectos PL puede relacionarse con SIL. Existen cinco niveles de rendimiento, PLa es el más bajo y PLe es el más alto.

Comparación de PL y SIL

Esta tabla muestra la relación aproximada entre PL y SIL cuando se aplica a estructuras de circuitos típicos logradas mediante tecnología electromecánica de baja complejidad.

PL (Nivel de rendimiento)	PFH_D (Probabilidad de fallos peligrosos por hora)	SIL (Nivel de integridad de seguridad)
A	$\geq 10^{-5}$ a $<10^{-4}$	Ninguno
B	$\geq 3 \times 10^{-6}$ a $<10^{-5}$	1
C	$\geq 10^{-6}$ a $<3 \times 10^{-6}$	1
D	$\geq 10^{-7}$ a $<10^{-6}$	2
E	$\geq 10^{-8}$ a $<10^{-7}$	3

Correspondencia aproximada entre PL y SIL

IMPORTANTE: *La tabla anterior se proporciona como orientación general y NO debe usarse para fines de conversión. Deben tenerse en cuenta los requisitos totales de los estándares.*

Diseño del sistema de acuerdo con IEC/EN 62061

IEC/EN 62061, “Seguridad de máquinas – Seguridad funcional de sistemas eléctricos, electrónicos y electrónicos programables relacionados con la seguridad” es la implementación específica de máquinas de IEC/EN 61508. Proporciona requisitos aplicables al diseño de nivel de sistema para todos los tipos de sistemas de control eléctrico relacionado a la seguridad de las máquinas y también para el diseño de subsistemas o dispositivos no complejos.

La evaluación de riesgos resulta en una estrategia de reducción de riesgos que a su vez identifica la necesidad de funciones de control con fines de seguridad. Estas funciones deben documentarse y deben incluir:

- especificación de requisitos funcionales
- especificación de requisitos de integridad de seguridad.

Los requisitos funcionales incluyen detalles como la frecuencia de operación, tiempo de respuesta requerido, modos de operación, ciclos de servicio, ambiente de operación y funciones de reacción ante fallo. Los requisitos de integridad de seguridad se expresan en niveles llamados niveles de integridad de seguridad (SIL). Según la complejidad del sistema, algunos o todos los elementos indicados en la siguiente tabla deberán considerarse para determinar si el diseño del sistema cumple con las especificaciones del nivel SIL requerido.

Elemento para consideración de nivel SIL	**Símbolo**
Probabilidad de fallos peligrosos por hora	PFH_D
Tolerancia a fallos de hardware	HFT
Fracción de fallo no peligroso	SFF
Intervalo de prueba de calidad	T1
Intervalo de prueba de diagnóstico	T2
Probabilidad de fallos por causas comunes	ß
Cobertura de diagnostico	DC

Elementos para consideración de nivel SIL

En los sistemas electrónicos, una contribución significativa a los fallos es el tiempo, comparado con el número de operaciones en el caso de los dispositivos electromecánicos. Por lo tanto se obtiene la tasa de fallo de los sistemas electrónicos en base al número de horas. Deberá realizarse un análisis de los componentes para determinar su probabilidad de fallo. Los sistemas de seguridad están interesados específicamente no solo en la probabilidad del fallo, sino lo que es más importante, la probabilidad de fallo a peligro en base al número de horas, el valor PFHD. Una vez que se conoce este valor, la siguiente tabla puede usarse para determinar cuál nivel SIL se logra.

SIL (Nivel de integridad de seguridad)	PFH_D (Probabilidad de fallos peligrosos por hora)
3	$\geq 10^{-8}$ a $<10^{-7}$
2	$\geq 10^{-7}$ a $<10^{-6}$
1	$\geq 10^{-6}$ a $<10^{-5}$

Probabilidades de fallo peligroso para los niveles SIL

El sistema de seguridad se divide en subsistemas. El nivel de integridad de seguridad de hardware que puede declararse para un subsistema está limitado por la tolerancia a fallo de hardware y la fracción de fallos no peligrosos del subsistema. La tolerancia a fallo de hardware es la capacidad del sistema de ejecutar su función en presencia de fallos. Una tolerancia a fallo de cero significa que la función no se realiza cuando se produce un fallo. Una tolerancia a fallo de uno permite que el subsistema realice su función en presencia de un solo fallo. La fracción de fallos no peligrosos es la porción de la tasa de fallos totales que no resulta en un fallo peligroso. La combinación de estos dos elementos se conoce como restricción de arquitectura y tiene la designación SILCL. La siguiente tabla muestra la relación de las restricciones de arquitecturas con respecto a SILCL.

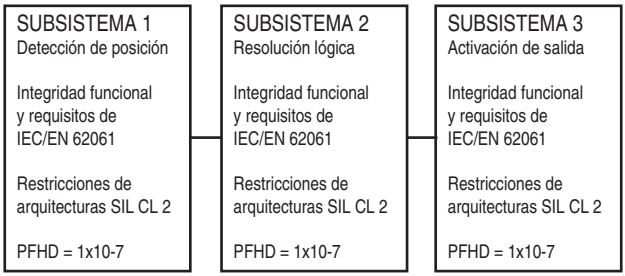
Fracción de fallo no peligroso (SFF)	Tolerancia a fallos de hardware		
	0	1	2
<60%	No permitido a menos que se apliquen excepciones específicas	SIL1	SIL2
60% – <90%	SIL1	SIL2	SIL3
90% – <99%	SIL2	SIL3	SIL3
≥99%	SIL3	SIL3	SIL3

Restricciones de arquitecturas con respecto a SIL

Por ejemplo, una arquitectura que posee tolerancia a un solo fallo y tiene una fracción de fallos no peligrosos de 75% está limitada a una clasificación no mayor que SIL2, independientemente de la probabilidad de fallo peligroso.

Para calcular la probabilidad de fallo peligroso, cada función de seguridad debe desglosarse en bloques de funciones, los cuales luego se ejecutan como subsistemas. El diseño de un sistema de muchas funciones de seguridad incluye un dispositivo detector conectado a un dispositivo lógico conectado a su vez a un accionador. Esto crea una configuración de subsistemas en serie. Si podemos determinar la probabilidad de fallo peligroso de cada

subsistema y conocemos su SILCL, entonces la probabilidad de fallo del sistema se calcula fácilmente sumando la probabilidad de fallos de los subsistemas. Este concepto se muestra a continuación.



= PFHD 1 + PFHD 2 + PFHD 3
= 1x10-7 + 1x10-7 + 1x10-7
= 3x10-7 es decir, idóneo para SIL2

Por ejemplo, si deseamos lograr el nivel SIL2, cada subsistema debe tener un límite de declaración de SIL (SIL CL) de por lo menos SIL2, y la suma de los valores de PFHD del sistema no debe superar el límite permitido en la tabla anterior que muestra la 'Probabilidad de fallos peligrosos para niveles SIL'.

El término "subsistema" tiene un significado especial en IEC/EN 62061. Es la subdivisión de primer nivel de un sistema en partes que, si fallan, causarían un fallo de la función de seguridad. Por lo tanto, si se usan dos interruptores redundantes en un sistema, ninguno de los interruptores individuales es un subsistema. El subsistema comprendería ambos interruptores y la función de diagnóstico de fallos asociada (si la hay).

Diseño del subsistema – IEC/EN 62061

Si un diseñador de sistema utiliza componentes ensamblados en subsistemas según IEC/EN 62061, las cosas se facilitan mucho porque no se aplican los requisitos específicos para el diseño de subsistemas. Estos requisitos serán cubiertos, en general, por el fabricante del dispositivo (subsistema) y son mucho más complejos que los requeridos para el diseño de nivel del sistema.

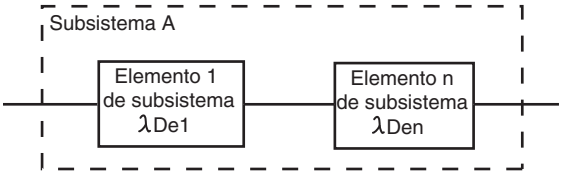
IEC/EN 62061 requiere que los subsistemas complejos, como los PLC de seguridad, cumplan con las especificaciones de IEC 61508. Esto significa que, para dispositivos que usan componentes complejos electrónicos o programables, está en pleno vigor el estándar IEC 61508. Esto puede ser un proceso muy difícil y laborioso. Por ejemplo, la evaluación de PFH_D lograda por un subsistema complejo puede ser un proceso complicado con técnicas tales como modelado Markov, diagramas de bloques de fiabilidad o análisis de árbol de fallos.

IEC/EN 62061 proporciona requisitos para el diseño de subsistemas de menor complejidad. Normalmente esto incluirá componentes eléctricos relativamente simples como interruptores

con enclavamiento y relés de control de seguridad electromecánicos. Los requisitos no son tan laboriosos como los de IEC 61508 pero pueden ser muy complicados.

IEC/EN 62061 proporciona cuatro arquitecturas lógicas de subsistemas, incluidas sus fórmulas, que pueden usarse para evaluar el PFHD logrado por un subsistema de baja complejidad. Estas arquitecturas son representaciones puramente lógicas y no deben considerarse arquitecturas físicas. En los siguientes cuatro diagramas se muestran las cuatro arquitecturas lógicas de subsistemas, incluidas sus fórmulas.

Para la arquitectura de subsistema básica mostrada a continuación, las probabilidades de fallos peligrosos simplemente se suman.



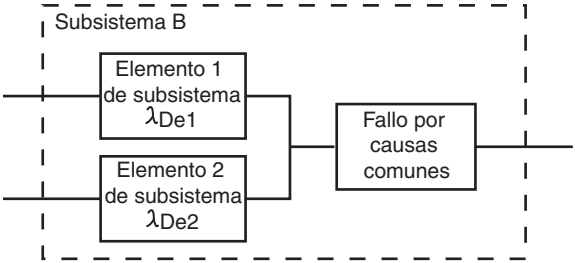
Arquitectura lógica de subsistema A

$\lambda_{DssA} = \lambda_{De1} + \ldots + \lambda_{Den}$

$PFH_{DssA} = \lambda_{DssA} \times 1h$

λ, Lambda se usa para designar la tasa de fallos. Las unidades de la tasa de fallos son fallos por hora. λ_D, Lambda sub D es la tasa de fallos peligrosos. λ_{DssA}, Lambda sub DssA es la tasa de fallos peligrosos del subsistema A. Lambda sub DssA es la suma de las tasas de fallos de los elementos individuales, e1, e2, e3, has en, incluyendo este último. La probabilidad de fallos peligrosos se multiplica por 1 hora para crear la probabilidad de fallo durante una hora.

El siguiente diagrama muestra un sistema tolerante a un solo fallo sin función de diagnósticos. Cuando la arquitectura incluye tolerancia a un solo fallo, existe el potencial de fallo por causas comunes y debe considerarse. La derivación del fallo por causas comunes se describe brevemente en este capítulo.



Arquitectura lógica de subsistema B

$\lambda_{DssB} = (1 - ß)^2 \times \lambda_{De1} \times \lambda_{De2} \times T_1 + ß \times (\lambda_{De1} + \lambda_{De2})/2$
$PFH_{DssB} = \lambda_{DssB} \times 1h$

Las fórmulas para esta arquitectura toman en consideración la configuración paralela de los elementos del subsistema y añaden los siguientes dos elementos de la tabla previa 'Elementos para consideración de SIL'.

ß – la probabilidad de fallos por causas comunes (Beta)

T1 – el intervalo de prueba de calidad o la vida útil, el menor de los dos. La prueba de calidad está diseñada para detectar fallos y la degradación del subsistema de seguridad de modo que el subsistema pueda restaurarse a una condición de operación.

Como ejemplo, suponga los siguientes valores:

ß = 0.10
$\lambda_{De1} = 1 \times 10^{-6}$ fallos/hora
$\lambda_{De2} = 1 \times 10^{-6}$ fallos/hora
T1 = 87600 horas (10 años)

La tasa de fallos del sistema es 1.70956E-07 fallos por hora (SIL2).

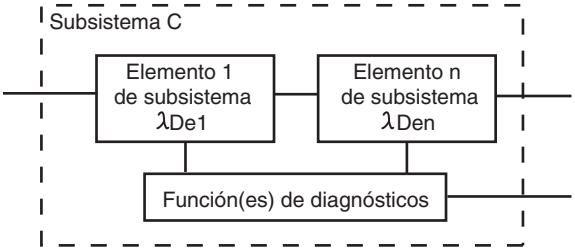
Efecto del intervalo de prueba de calidad

Examinemos el efecto que el intervalo de prueba de calidad tiene en el sistema. Suponga que el intervalo de prueba de calidad se redujo a dos veces al año. Esto reduce T1 a 4380 horas y la tasa de fallos peligrosos mejora a 1.03548E-07 fallos por hora. Esto todavía es sólo SIL2. Si el intervalo de prueba de calidad se reduce a mensual (730 horas), la tasa de fallos peligrosos mejora a 1.0059E-07 fallos por hora. Esto todavía es sólo SIL2. Se necesita una mejora adicional en tasa de fallos, intervalo de prueba de calidad o fallo por causas comunes para lograr la clasificación SIL3. Además, el diseñador debe mantener en consideración que el subsistema debe combinarse con otros subsistemas para calcular la tasa total de fallos peligrosos.

Efecto del análisis de fallo por causas comunes

Examinemos el efecto que el fallo por causas comunes tiene en el sistema. Suponga que tomamos medidas adicionales y nuestro valor beta mejora a su mejor nivel de 1% (0,01), mientras que el intervalo de prueba de calidad permanece en 10 años. La tasa de fallos peligrosos mejora a 9.58568E-08. El sistema ahora cumple con la clasificación SIL3.

El siguiente diagrama muestra la representación funcional de un sistema tolerante a cero fallos con una función de diagnósticos. La cobertura de diagnósticos se usa para reducir la probabilidad de fallos de hardware peligrosos. Las pruebas de diagnóstico se realizan automáticamente. La cobertura de diagnósticos es la relación de la tasa de fallos peligrosos detectados comparado con la tasa de todos los fallos peligrosos. El tipo o número de fallos no peligrosos no se considera al calcular la cobertura de diagnósticos; sólo es el porcentaje de fallos peligrosos detectados.



Arquitectura lógica de subsistema C

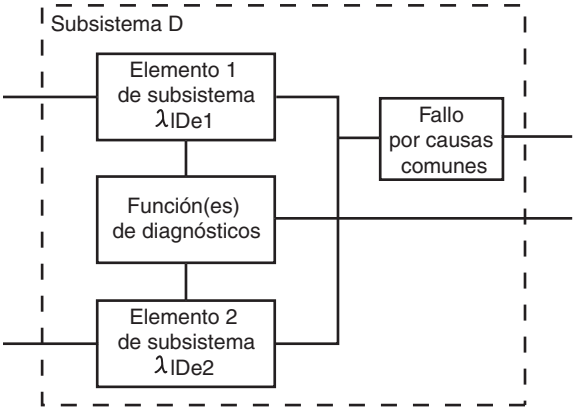
$$\lambda_{DssC} = \lambda_{De1} (1 - DC_1) + \ldots + \lambda_{Den} (1 - DC_n)$$
$$PFH_{DssC} = \lambda_{DssC} \times 1h$$

Estas fórmulas incluyen la cobertura de diagnósticos, DC, para cada elemento del subsistema. Las tasas de fallos de cada uno de los subsistemas se reduce por la cobertura de diagnostico de cada subsistema.

A continuación se muestra el cuarto ejemplo de una arquitectura de subsistemas. Este subsistema es tolerante a un solo fallo e incluye una función de diagnóstico. El potencial de fallo por causas comunes también debe considerarse en los sistemas tolerantes a un solo fallo.

Si los elementos del subsistema son los mismos, se usan las siguientes fórmulas:

$$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De}^2 \times 2 \times DC \times T_2/2 + \lambda_{De}^2 \times (1 - DC) \times T_1 \} + ß \times \lambda_{De}$$
$$PFH_{DssD} = \lambda_{DssD} \times 1h$$



Arquitectura lógica de subsistema D

Si los elementos del subsistema son diferentes, se usan las siguientes fórmulas:

$$\lambda_{DssD} = (1 - ß)^2 \{ \lambda_{De1} \times \lambda_{De2} \times (DC_1 + DC_2) \times T_2/2 + \lambda_{De1} \times \lambda_{De2} \times (2 - DC_1 - DC_2) \times T_1/2 \} + ß \times (\lambda_{De1} + \lambda_{De2})/2$$

$$PFH_{DssD} = \lambda_{DssD} \times 1h$$

Observe que ambas fórmulas usan un parámetro adicional, T2 el intervalo de diagnóstico.

Como ejemplo, suponga los siguientes valores para el ejemplo donde los elementos del subsistema son diferentes:

ß = 0.10
$\lambda_{De1} = 1 \times 10^{-6}$ fallos/hora
$\lambda_{De2} = 2 \times 10^{-6}$ fallos/hora
T1 = 87600 horas (10 años)
T2 = 876 horas
DC1 = 0,8
DC2 = 0,6

PFH_{DssD} = 2.36141E-07 fallos peligrosos por hora

Metodología de transición para categorías

Durante la escritura de IEC/EN 62061, el comité reconoció que se necesitaría un tiempo considerable para que todos los datos requeridos para los sistemas y dispositivos estén completamente disponibles. Se incluyeron dos tablas para ayudar a convertir los diseños de subsistemas existentes basados en el concepto original de categorías con uso eficaz comprobado. Ellos proporcionan la equivalencia para PFH_D y restricciones de arquitecturas. Las tablas facilitan una ruta de transición útil a los estándares de seguridad funcional. Las tablas se han simplificado ligeramente en este documento. Si se estudian, será evidente que las arquitecturas de los diversos ejemplos de sistema de categorías proporcionados en capítulos anteriores pueden retenerse bajo el concepto de estándares de seguridad funcional.

Categoría	Tolerancia a fallos	Cobertura de diagnostico	PFH_D que puede declararse para el subsistema
1	0	0%	Consulte IEC/EN 62061
2	0	60% – 90%	$\geq 10^{-6}$
3	1	60% – 90%	$\geq 2 \times 10^{-7}$
4	>1	60% – 90%	$\geq 3 \times 10^{-8}$
	1	>90%	$\geq 3 \times 10^{-8}$

Declaración de PFHD basada en categoría

La tabla anterior 'Restricciones de arquitecturas con respecto a SIL' es una versión simplificada de la Tabla 7 del estándar. Use esta tabla cuando un subsistema basado en categorías se convierte en parte de SRCS que debe cumplir con las especificaciones de IEC/EN 62061. Por razones de simplicidad, el diseñador del sistema de seguridad puede declarar un PFH_D de 2×10^{-7} para un sistema basado en la categoría 3 que cuenta con una cobertura de diagnósticos del 60%. Alternativamente, el diseñador del sistema de seguridad puede realizar un análisis completo si por la determinación puede declararse un mejor valor PFHD.

Categoría	Tolerancia a fallos	SFF	Límite máximo de declaración de SIL según restricciones de la arquitectura
1	0	<60%	Consulte IEC/EN 62061
2	0	60% – 90%	SIL1
3	1	<60%	SIL1
	1	60% – 90%	SIL2
4	>1	60% – 90%	SIL3

Restricciones de arquitecturas basadas en categorías

La tabla 'Declaración de valor PFHD basada en categorías' puede usarse para determinar el límite de declaración SIL de un subsistema basado en categorías. La cobertura de diagnósticos del sistema basado en categorías debe convertirse a fracción de fallos no peligrosos.

Al conocer los valores PFH_D y SIL CL de un sistema basado en categorías, el diseñador del sistema de seguridad puede aplicar estos valores en uno de los subsistemas mostrados anteriormente. Si el sistema basado en categorías es el SRCS completo, entonces los equivalentes de SIL y PFH_D son determinados por las tablas 'Restricciones de arquitecturas con respecto a SIL' y la 'Declaración de PFHD basado en categorías'. El diseñador del sistema de seguridad también debe satisfacer los requisitos de fallos por causas comunes, fallos sistemáticos e intervalo de prueba de calidad. El sistema de puntuación para fallos por causas comunes es ligeramente diferente para cada estándar. Los conceptos para la integridad de la seguridad sistemática son similares en ambos estándares; ninguno de los estándares utiliza un sistema de puntuación. El intervalo de prueba de calidad puede considerarse igual que el tiempo de misión, o puede seleccionarse un intervalo más corto.

Restricciones de arquitecturas

El nivel de integridad de seguridad que se puede declarar para un sistema o subsistema está limitado a las características de la arquitectura. Las dos características primarias son tolerancia a fallos de hardware y fracción de fallos no peligrosos. Las características secundarias incluyen fallos por causas comunes y exclusión de fallos.

Al combinar subsistemas, el SIL logrado por el SRCS está restringido a menos o igual que el límite de declaración de SIL de cualquiera de los subsistemas incluidos en la función de control relacionada a la seguridad.

B10 y $B10_d$

Para los subsistemas electromecánicos, la probabilidad de fallo debe calcularse considerando el número de ciclos de operación declarado por el fabricante, la carga y el ciclo de servicio. La probabilidad de fallo se expresa como el valor B10, el cual es el tiempo esperado al cual fallará el 10% de la población. $B10_d$ es el tiempo esperado al cual fallará a peligro el 10% de la población.

Fallo por causas comunes (CCF)

El fallo por causas comunes es cuando múltiples fallos que son resultado de una sola causa producen un fallo peligroso. La información sobre CFF generalmente sólo será requerida por el diseñador del subsistema, generalmente el fabricante. Se usa como parte de las fórmulas dadas para el cálculo del valor PFHD de un subsistema. Generalmente no se requerirá a nivel de diseño del sistema. El Anexo F de IEC/EN 62061 proporciona un método simple para calcular el CCF. La siguiente tabla muestra un resumen del proceso de puntaje.

Núm.	Medida contra CCF	Puntaje
1	Separación/segregación	25
2	Diversidad	38
3	Diseño/aplicación/experiencia	2
4	Evaluación/análisis	18
5	Capacitación/formación técnica	4
6	Condiciones ambientales	18

Puntaje para medidas contra el fallo por causas comunes

Se otorgan puntos para emplear medidas especificas contra el CCF. Los puntos se suman para determinar el factor de fallo por causas comunes, el cual se muestra en la siguiente tabla. El factor beta se usa en modelos de subsistemas para “ajustar” la tasa de fallos.

Puntaje total	Factor de fallo por causas comunes (ß)
<35	10% (0,1)
35 – 65	5% (0,05)
65 – 85	2% (0,02)
85 – 00	1% (0,01)

Factor beta para fallo por causas comunes

Cobertura de diagnósticos (DC)

Las pruebas de diagnóstico automáticas se emplean para reducir la probabilidad de fallos peligrosos de hardware. Sería ideal poder detectar el 100% de los fallos de hardware peligrosos, pero esto generalmente es difícil de lograr.

La cobertura de diagnósticos es la relación de los fallos peligrosos detectados comparado con todos los fallos peligrosos.

$$DC = \frac{\text{Tasa de fallos peligrosos detectados, } \lambda_{DD}}{\text{Tasa de fallos peligrosos totales, } \lambda_{Dtotal}}$$

El valor de la cobertura de diagnósticos será entre cero y uno.

Tolerancia a fallos de hardware

La tolerancia a fallos de hardware representa el número de fallos que un subsistema puede sostener antes de que se produzca un fallo peligroso. Por ejemplo, una tolerancia a fallos de hardware de 1 significa que 2 fallos causarían una pérdida de la función de control de seguridad, pero no un fallo.

Gestión de la seguridad funcional

El estándar proporciona requisitos para el control de gestión y las actividades técnicas necesarias para lograr un sistema de control eléctrico relacionado con la seguridad.

Probabilidad de daño peligroso (PFH_D)

Parte de los requisitos necesarios para lograr cualquier capacidad SIL para un sistema o subsistema son los datos sobre PFH_D (probabilidad de un fallo peligroso por hora) debido a fallo de hardware aleatorio.

Estos datos serán proporcionados por el fabricante. Ya están disponibles los datos para los nuevos componentes y sistemas de seguridad de Rockwell Automation (por ej., GuardLogix, GuardPLC, SmartGuard y Kinetix con GuardMotion, interruptores de enclavamiento, paros de emergencia, etc.).

IEC/EN 62061 también indica que los manuales de datos de fiabilidad pueden usarse cuando corresponde.

Para dispositivos electromecánicos de baja complejidad, el mecanismo de fallo generalmente está vinculado al número y frecuencia de operaciones, y no sólo al tiempo. Por lo tanto, para estos componentes los datos serán determinados a partir de alguna forma de prueba de vida útil (por ej., la prueba B10). B10 es la información basada en la aplicación sobre el número de operaciones, tal como el número de operaciones previstas por año que se requiere para convertir el dato de $B10_d$ o datos similares a $MTTF_d$ (tiempo medio para fallo peligroso). Este dato a su vez, se convierte a PFH_D.

En general se puede asumir lo siguiente:

$$PFH_D = 1/MTTF_d$$

Y para dispositivos electromecánicos:

$$MTTF_d = B_{10d}/(0.1 \times \text{número medio de operaciones por año})$$

La fórmula de $MTTF_d$ se basa en la suposición de la tasa de fallo constante. La distribución de fallos acumulados es $F(t) = 1 - \exp(-\lambda dt)$.

Intervalo de prueba de calidad

El intervalo de prueba de calidad representa el tiempo después del cual un subsistema debe verificarse o reemplazarse totalmente para asegurar que quede en una condición “como nuevo”. En la práctica, en el sector de máquinas, esto se realiza mediante el reemplazo. Por lo tanto, el intervalo de prueba de calidad generalmente es igual que la vida útil. EN ISO 13849-1:2008 se refiere a ello como tiempo de misión.

Una prueba de calidad es una verificación que puede detectar fallos y degradación en un SRCS de modo que el SRCS pueda restaurarse una condición de “como nuevo”. La prueba de calidad debe detectar el 100% de todos los fallos peligrosos. Los diferentes canales deben probarse por separado.

A diferencia de las pruebas de diagnóstico que son automáticas, las pruebas de calidad generalmente se realizan manualmente y fuera de línea. Por ser automáticas, las pruebas de diagnóstico se realizan a menudo comparado con las pruebas de calidad que se hacen con poca frecuencia. Por ejemplo, los circuitos que van a un interruptor de enclavamiento en una guarda pueden probarse automáticamente para detectar condiciones de cortocircuito y circuito abierto con pruebas de diagnóstico (por ej., impulsos).

El intervalo de prueba de calidad debe ser declarado por el fabricante. Algunas veces el fabricante proporciona un rango diferente de intervalos de prueba de calidad. El intervalo de prueba de calidad se determina mediante una revisión de las fórmulas para la arquitectura seleccionada. En general, cuanto más corto es el intervalo de prueba de calidad, más baja la tasa de fallos.

Fracción de fallo no peligroso (SFF)

La fracción de fallo no peligroso es similar a la cobertura de diagnóstico, pero también toma en consideración cualquier tendencia inherente a fallo a un estado de seguridad. Por ejemplo, cuando se funde un fusible hay un fallo, pero es muy probable que el fallo sea un circuito abierto que, en la mayoría de casos sería un fallo “no peligroso”. SFF es (la suma de la tasa de fallos “no peligrosos” más la tasa de fallos peligrosos detectados) dividido entre (la suma de la tasa de fallos “no peligrosos” más la tasa de fallos peligrosos detectados y no detectados). Es importante anotar que los únicos tipos de fallos a considerar son aquellos que podrían tener algún efecto en la función de seguridad.

La mayoría de dispositivos mecánicos de baja complejidad, tales como botones de paro de emergencia e interruptores de enclavamiento (por ellos mismos) tendrán un SFF de menos del 60%, pero la mayoría de dispositivos electrónicos por seguridad tienen redundancia y monitorización en su diseño, por lo tanto un SFF de más del 90% es común. El valor de SFF normalmente lo proporcionará el fabricante.

La fracción de fallo no peligroso (SFF) puede calcularse mediante la siguiente ecuación:

$$SFF = (\Sigma\lambda_S + \Sigma\lambda_{DD})/(\Sigma\lambda_S + \Sigma\lambda_D)$$

donde

λ_S = la tasa de fallo no peligroso,

$\Sigma\lambda_S + \Sigma\lambda_D$ = la tasa de fallos totales,

λ_{DD} = la tasa de fallos peligrosos detectados,

λ_D = la tasa de fallos peligrosos.

Fallo sistemático

El estándar tiene requisitos para el control y prevención de fallos sistemáticos. Los fallos sistemáticos son diferentes a los fallos de hardware aleatorios, que son fallos que ocurren en momentos aleatorios, generalmente como resultado de la degradación de piezas de hardware. Los tipos típicos de posibles fallos sistemáticos son errores de diseño de software, errores de diseño de hardware, errores de especificación de requisitos y procedimientos de operación. Algunos ejemplos de pasos necesarios para evitar un fallo sistemático son:

- correcta selección, combinación, configuraciones, ensamblaje e instalación de componentes;
- use de buenas prácticas de ingeniería;
- seguir las especificaciones del fabricante y las instrucciones de instalación;
- asegurar la compatibilidad entre los componentes
- resistencia de las condiciones ambientales
- use de materiales apropiados

El estándar proporciona requisitos adicionales y más detallados necesarios para evitar los fallos sistemáticos. El estándar no contiene un sistema de puntuación para determinar cuál porcentaje de fallos sistemáticos potenciales se cubren. Para satisfacer los requisitos de SIL3, el diseñador debe satisfacer todos los requisitos para evitar los fallos sistemáticos. Si no se cumplen todos los requisitos, entonces deberá reducirse el límite de declaración de SIL.

Diseño del sistema de acuerdo con EN ISO 13849-1:2008

Se requiere un estudio completo y detallado de EN ISO 13849-1:2008 para poder aplicarlo correctamente. La siguiente es una descripción general breve:

Este estándar proporciona requisitos para el diseño e integración de las partes relacionadas a la seguridad de los sistemas de control e incluye algunos aspectos de software. El estándar se aplica a un sistema relacionado con la seguridad, pero también puede aplicarse a los componentes el sistema. Este estándar también tiene amplia capacidad de aplicación ya que se usa en todas las tecnologías, inclusive sistemas eléctricos, hidráulicos, neumáticos y mecánicos. Aunque el estándar ISO 13849-1 se aplica a sistemas complejos, dirige al lector a los estándares IEC 62061 e IEC 61508 para sistemas incorporados de software complejos.

Con ese estándar, la integridad de la seguridad de un sistema se clasifica en 5 PLs (niveles de rendimiento). PLa es la integridad más baja y PLe es la integridad más alta. Estos se evalúan tomando en cuenta los siguientes factores:

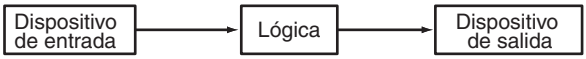
Estructura (arquitectura). Están directamente relacionados con las categorías descritas anteriormente en este documento.

Tiempo de misión – vida operativa prevista
MTTFd – tiempo medio para fallo peligroso
DC – cobertura de diagnostico
CCF – fallo por causas comunes
Comportamiento bajo condiciones de fallo
Software
Fallos sistemáticos
Condiciones ambientales

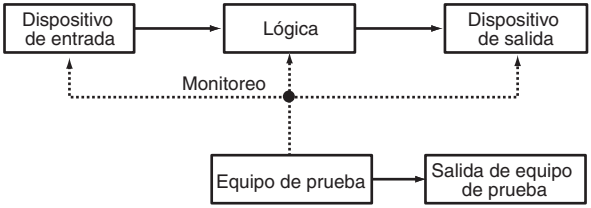
Arquitecturas (estructuras) del sistema de seguridad

El estándar proporciona un procedimiento simplificado basado en categorías para calcular el PL. La intención de esta estrategia es proporcionar una ruta de transición reconocible desde el estándar original basado en categorías hasta la versión 2006 basada en nivel de rendimiento. El estándar proporciona 5 arquitecturas designadas como se muestra a continuación. Corresponden a las 5 categorías existentes B, 1, 2, 3 y 4. Estos diagramas deben estudiarse detalladamente en la cláusula 6 del estándar, donde se explican los requisitos, diferencias y suposiciones. Los diagramas de arquitectura para las categorías B y 1, y también 3 y 4, pueden parecer iguales, pero el estándar explica las diferencias en detalle en términos de sus requisitos, incluso la cobertura de diagnóstico.

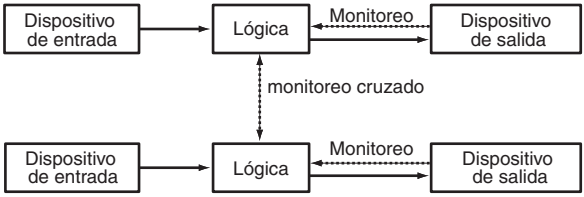
También será útil estudiar la explicación de las categorías proporcionadas en esta publicación y que describe las categorías en detalle con ejemplos prácticos de su implementación. Los siguientes tres diagramas muestran los diagramas de bloques de las arquitecturas de categoría 5, como se muestra en ISO/EN 13849-1.



Arquitectura designada para la Categoría B y 1



Arquitectura designada para la Categoría 2



Arquitectura designada para la Categoría 3 y 4

Tiempo de misión

El tiempo de misión representa el período de tiempo máximo que puede usarse un subsistema (o sistema). Después de este tiempo, debe reemplazarse. El tiempo de misión debe ser declarado por el fabricante de los componentes. El tiempo de misión generalmente será igual que el del “intervalo de prueba de calidad” usado en IEC/EN 62061. El diseñador del sistema de seguridad entonces debe considerar el tiempo de misión de los componentes para determinar el tiempo de misión de cada función de seguridad.

Tiempo medio para fallo peligroso ($MTTF_d$)

El $MTTF_d$ (tiempo medio para fallo peligroso) se usa directamente en EN ISO 13849-1:2008 como parte del cálculo del PL. El estándar ofrece tres métodos para determinar el $MTTF_d$: 1) usar datos del fabricante, 2) usar los Anexos C y D que proporcionan tasas de fallo de componentes, o 3) usar un valor predeterminado de 10 años. Seleccionar el valor predeterminado restringe el rango a Medio como se muestra en la siguiente tabla.

Denotación de MTTFd de cada canal	Rango de MTTFd de cada canal
Bajo	3 años <= MTTFd <10 años
Mediano	10 años <= MTTFd <30 años
Alto	30 años <= MTTFd <100 años

Niveles de $MTTF_d$

Cuando el sistema de seguridad implica interfaz con IEC 62061, el valor de $MTTF_d$ debe convertirse en PFH_D. Esto se realiza mediante la siguiente relación:

$$PFH_D = 1/MTTF_d$$

Y para dispositivos electromecánicos:

$$MTTF_d = B10_d/(0.1 \times \text{número medio de operaciones por año})$$

En algunos casos también se requiere la determinación de PFH_D. Éste valor será proporcionado por los fabricantes. El valor de $MTTF_d$ y PFH_D generalmente se determina a partir de la misma fuente de prueba o análisis de datos. Para dispositivos electromecánicos de baja complejidad, el mecanismo de fallo generalmente está vinculado al número y frecuencia de operaciones, y no sólo al tiempo. Por lo tanto, para estos componentes los datos se determinarán a partir de alguna forma de prueba de vida útil (por ej., la prueba B10). A continuación se requiere la información basada en la aplicación, como el número previsto de operaciones por año, para convertir el valor $B10_d$ o un dato similar a $MTTF_d$.

Cobertura de diagnósticos (DC)

La cobertura de diagnósticos (DC) representa la eficacia de la monitorización de fallos de un sistema o subsistema. DC es la relación entre la tasa de fallos de los fallos peligrosos detectados y la tasa de fallos del total de fallos peligrosos. EN ISO 13849-1:2008 y IEC 61508 proporciona tablas que pueden usarse para determinar el valor de DC y en algunos casos el valor DC puede ser proporcionado por los fabricantes.

Fallo por causas comunes (CCF)

El fallo por causas comunes (CFF) ocurre cuando múltiples fallos que son resultado de una sola causa producen un fallo peligroso. Estos son fallos de diferentes componentes que resultan de un solo evento. Los fallos no son consecuencia uno de otro. El Anexo F de EN ISO 13849-1:2008 proporciona un método cualitativo simplificado de determinar el CCF. La siguiente tabla muestra un resumen del proceso de puntaje.

Núm.	Medida contra CCF	Puntaje
1	Separación/segregación	15
2	Diversidad	20
3	Diseño/aplicación/experiencia	20
4	Evaluación/análisis	5
5	Capacitación/formación técnica	5
6	Condiciones ambientales	35

Puntaje para fallo por causas comunes

Debe obtenerse una puntuación de por lo menos 65 para declarar conformidad según las categorías 2, 3 y 4.

Fallo sistemático

Los estándares tienen requisitos para el control y prevención de fallos sistemáticos. Los tipos típicos de posibles fallos sistemáticos son errores de diseño de software, errores de diseño de hardware, errores de especificación de requisitos.

Los fallos sistemáticos son diferentes a los fallos de hardware aleatorios, que son fallos que ocurren en momentos aleatorios, generalmente como resultado de la degradación de piezas de hardware. El Anexo G de EN ISO 13849-1:2008 describe las medidas para el control y prevención de fallos sistemáticos.

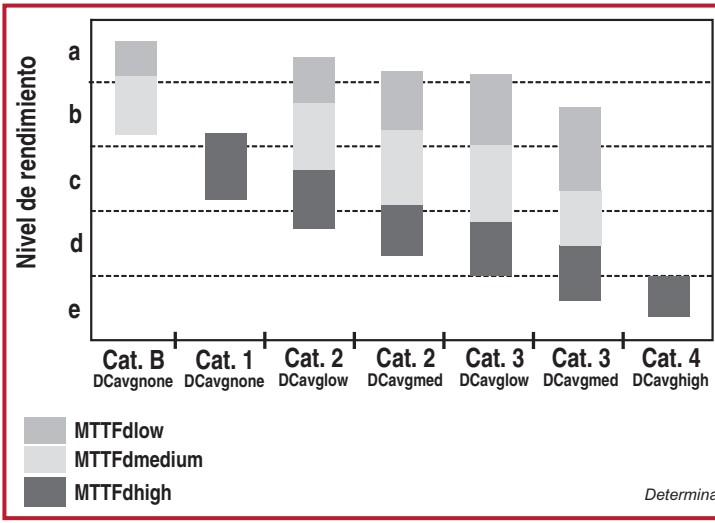
Nivel de rendimiento (PL)

Al evaluar los criterios de diseño en la tabla anterior que muestra 'Niveles de $MTTD_d$', se asignará al SRCS un nivel de rendimiento. El nivel de rendimiento es un nivel discreto que especifica la capacidad de un sistema de control de realizar una función de seguridad en sus partes relacionadas con esta misma seguridad.

Para evaluar el PL logrado por una implementación de cualquiera de las 5 arquitecturas designadas, se requieren los siguientes datos del sistema (o subsistema):

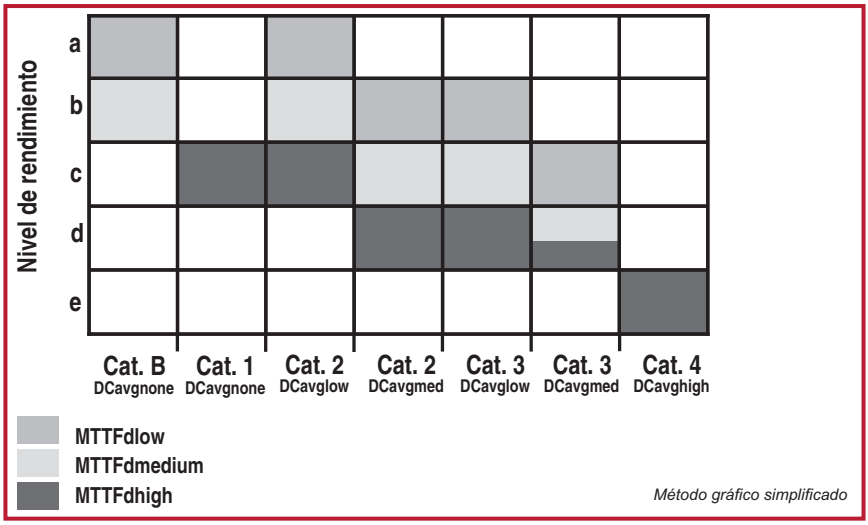
- $MTTF_d$ (tiempo medio para fallo peligroso de cada canal)
- DC (cobertura de diagnóstico)
- Arquitectura (la categoría)

El siguiente diagrama muestra un método gráfico para determinar el PL a partir de una combinación de estos factores. La tabla al final de esta sección muestra los resultados tabulares de diferentes modelos Markov que crearon la base de este diagrama. Consulte la tabla cuando necesite determinaciones más precisas.



Determinación gráfica de PL

El lector observará que existe alguna superposición en las líneas de división de PL. Si MTTF sólo se proporciona en términos categóricos (como bajo, medio o alto), use el siguiente diagrama para determinar el PL.



Por ejemplo, una aplicación usa la arquitectura designada de Categoría 3. Si DC está entre el 60% y el 90%, y el valor de $MTTF_d$ de cada canal es entre 10 y 30 años, entonces según la Figura 10.7, se obtiene PLd.

Otros factores también deben ejecutarse para satisfacer el PL requerido. Estos requisitos incluyen provisiones para fallos por causas comunes, fallo sistemático, condiciones ambientales y tiempo de misión.

Si el PFH_D del sistema o subsistema se conoce, puede usarse la Tabla 10.4 (Anexo K del estándar) para determinar el PL.

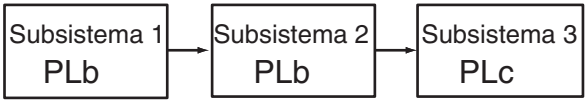
Diseño y combinaciones de subsistemas

Los subsistemas que cumplen con las especificaciones de un PL pueden combinarse de manera simple en un sistema mediante la Tabla 10.3. La razón de esta tabla es clara. Primero, que el sistema solo puede ser tan bueno como su subsistema más débil. Segundo, cuanto más subsistemas hayan, mayor será la posibilidad de fallo.

PL_{low}	N_{low}	PL
a	>3	no permitido
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Cálculo de PL para subsistemas combinados en serie

En el sistema mostrado en el siguiente diagrama de yjr, los niveles de rendimiento más bajos están en los subsistemas 1 y 2. Ambos son PLb. Por lo tanto, al usar esta tabla podemos leer horizontalmente b (en la columna PL_{low}), hasta 2 (en la columna N_{low}) y encontrar el PL del sistema como b (en la columna PL). Si todos los subsistemas tuvieran el nivel PLb, el PL logrado sería PLa.



Combinación de subsistemas en serie como un sistema PLb

Validación

La validación desempeña un papel importante en todo el proceso de desarrollo y puesta en marcha del sistema de seguridad. ISO/EN 13849-2:2003 establece los requisitos para la validación de sistemas diseñados según el estándar original ISO 13849-1 (EN 954-1). Se prevé que este estándar será revisado para ponerlo en línea con el estándar EN ISO 13849-1:2008 de sistemas diseñados según EN ISO 13849-1:2008. La validación por ISO 13849-2 requiere un plan de validación y describe la validación mediante técnicas de prueba y análisis tales como análisis de árbol de fallos y modos de fallo, análisis de efectos y criticidad. La mayoría de estos requisitos regirán para el fabricante del subsistema y no para el usuario del subsistema.

Puesta en marcha de la máquina

En la etapa de puesta en marcha del sistema o de la máquina, debe llevarse a cabo la validación de todas las funciones de seguridad en todos los modos de operación, y debe cubrir todas las condiciones anormales previsibles. También deben considerarse las combinaciones de entradas y las secuencias de operación. Este procedimiento es importante porque siempre es necesario verificar que el sistema sea idóneo para las características de operación y ambientales reales.

Algunas de estas características pueden ser diferentes de las previstas en la etapa de diseño.

Exclusión de fallo

Una de las principales herramientas de análisis para sistemas de seguridad es el análisis de fallos. El diseñador y el usuario deben entender cómo se desempeña el sistema de seguridad en la presencia de fallos. Hay muchas técnicas disponibles para realizar el análisis. Algunos ejemplos son análisis de árbol de fallos, modos de fallo, análisis de efectos y criticidad, análisis de árbol de eventos y análisis de carga y fuerza.

Durante el análisis, es posible que se descubran algunos fallos que no pueden detectarse con pruebas automáticas de diagnostico sin un coste económico excesivo. Más aún, la probabilidad de que ocurran estos fallos puede ser extremadamente baja al usar diseño de mitigación, construcción y métodos de prueba. Bajo estas condiciones, puede excluirse una mayor consideración de los fallos. Exclusión de un fallo significa descartar la ocurrencia de un fallo porque la probabilidad de que se produzca dicho fallo del SRCS es insignificante.

EN ISO 13849-1:2008 permite la exclusión de un fallo en base a la improbabilidad técnica de ocurrencia, la experiencia técnica generalmente aceptada y los requisitos técnicos relacionados con la aplicación. ISO 13849-2:2003 proporciona ejemplos y justificaciones para excluir ciertos fallos en los sistemas eléctricos, neumáticos, hidráulicos y mecánicos. La exclusión de fallos debe declararse con justificaciones detalladas provistas en la documentación técnica.

La exclusión de fallos puede conducir a un PL muy alto. Deben aplicarse medidas apropiadas para permitir esta exclusión de fallos durante el tiempo de misión completo. No siempre es posible evaluar SRCS sin suponer que ciertos fallos pueden excluirse. Para obtener información detallada sobre las exclusiones de fallos, consulte ISO 13849-2.

MTTFd para cada canal en años	Probabilidad promedio de fallos peligroso por hora (1/h) y nivel de rendimiento correspondiente (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = ninguno		DC_{avg} = ninguno		DC_{avg} = bajo		DC_{avg} = medio		DC_{avg} = bajo		DC_{avg} = medio		DC_{avg} = alto	
3	$3{,}80 \times 10^{-5}$	a			$2{,}58 \times 10^{-5}$	a	$1{,}99 \times 10^{-5}$	a	$1{,}26 \times 10^{-5}$	a	$6{,}09 \times 10^{-6}$	b		
3,3	$3{,}46 \times 10^{-5}$	a			$2{,}33 \times 10^{-5}$	a	$1{,}79 \times 10^{-5}$	a	$1{,}13 \times 10^{-5}$	a	$5{,}41 \times 10^{-6}$	b		
3,6	$3{,}17 \times 10^{-5}$	a			$2{,}13 \times 10^{-5}$	a	$1{,}62 \times 10^{-5}$	a	$1{,}03 \times 10^{-5}$	a	$4{,}86 \times 10^{-6}$	b		
3,9	$2{,}93 \times 10^{-5}$	a			$1{,}95 \times 10^{-5}$	a	$1{,}48 \times 10^{-5}$	a	$9{,}37 \times 10^{-6}$	b	$4{,}40 \times 10^{-6}$	b		
4,3	$2{,}65 \times 10^{-5}$	a			$1{,}76 \times 10^{-5}$	a	$1{,}33 \times 10^{-5}$	a	$8{,}39 \times 10^{-6}$	b	$3{,}89 \times 10^{-6}$	b		
4,7	$2{,}43 \times 10^{-5}$	a			$1{,}60 \times 10^{-5}$	a	$1{,}20 \times 10^{-5}$	a	$7{,}58 \times 10^{-6}$	b	$3{,}48 \times 10^{-6}$	b		
5,1	$2{,}24 \times 10^{-5}$	a			$1{,}47 \times 10^{-5}$	a	$1{,}10 \times 10^{-5}$	a	$6{,}91 \times 10^{-6}$	b	$3{,}15 \times 10^{-6}$	b		
5,6	$2{,}04 \times 10^{-5}$	a			$1{,}33 \times 10^{-5}$	a	$9{,}87 \times 10^{-6}$	b	$6{,}21 \times 10^{-6}$	b	$2{,}80 \times 10^{-6}$	c		
6,2	$1{,}84 \times 10^{-5}$	a			$1{,}19 \times 10^{-5}$	a	$8{,}80 \times 10^{-6}$	b	$5{,}53 \times 10^{-6}$	b	$2{,}47 \times 10^{-6}$	c		
6,8	$1{,}68 \times 10^{-5}$	a			$1{,}08 \times 10^{-5}$	a	$7{,}93 \times 10^{-6}$	b	$4{,}98 \times 10^{-6}$	b	$2{,}20 \times 10^{-6}$	c		
7,5	$1{,}52 \times 10^{-5}$	a			$9{,}75 \times 10^{-6}$	b	$7{,}10 \times 10^{-6}$	b	$4{,}45 \times 10^{-6}$	b	$1{,}95 \times 10^{-6}$	c		
8,2	$1{,}39 \times 10^{-5}$	a			$8{,}87 \times 10^{-6}$	b	$6{,}43 \times 10^{-6}$	b	$4{,}02 \times 10^{-6}$	b	$1{,}74 \times 10^{-6}$	c		
9,1	$1{,}25 \times 10^{-5}$	a			$7{,}94 \times 10^{-6}$	b	$5{,}71 \times 10^{-6}$	b	$3{,}57 \times 10^{-6}$	b	$1{,}53 \times 10^{-6}$	c		
10	$1{,}14 \times 10^{-5}$	a			$7{,}18 \times 10^{-6}$	b	$5{,}14 \times 10^{-6}$	b	$3{,}21 \times 10^{-6}$	b	$1{,}36 \times 10^{-6}$	c		
11	$1{,}04 \times 10^{-5}$	a			$6{,}44 \times 10^{-6}$	b	$4{,}53 \times 10^{-6}$	b	$2{,}81 \times 10^{-6}$	c	$1{,}18 \times 10^{-6}$	c		
12	$9{,}51 \times 10^{-5}$	b			$5{,}84 \times 10^{-6}$	b	$4{,}04 \times 10^{-6}$	b	$2{,}49 \times 10^{-6}$	c	$1{,}04 \times 10^{-6}$	c		
13	$8{,}78 \times 10^{-5}$	b			$5{,}33 \times 10^{-6}$	b	$3{,}64 \times 10^{-6}$	b	$2{,}23 \times 10^{-6}$	c	$9{,}21 \times 10^{-7}$	d		
15	$7{,}61 \times 10^{-6}$	b			$4{,}53 \times 10^{-6}$	b	$3{,}01 \times 10^{-6}$	b	$1{,}82 \times 10^{-6}$	c	$7{,}44 \times 10^{-7}$	d		
16	$7{,}31 \times 10^{-6}$	b			$4{,}21 \times 10^{-6}$	b	$2{,}77 \times 10^{-6}$	c	$1{,}67 \times 10^{-6}$	c	$6{,}76 \times 10^{-7}$	d		

MTTFd para cada canal en años	Probabilidad promedio de fallos peligroso por hora (1/h) y nivel de rendimiento correspondiente (PL)													
	Cat. B	PL	Cat. 1	PL	Cat. 2	PL	Cat. 2	PL	Cat. 3	PL	Cat. 3	PL	Cat. 4	PL
	DC_{avg} = ninguno		DC_{avg} = ninguno		DC_{avg} = bajo		DC_{avg} = medio		DC_{avg} = bajo		DC_{avg} = medio		DC_{avg} = alto	
18	$6{,}34 \times 10^{-6}$	b			$3{,}68 \times 10^{-6}$	b	$2{,}37 \times 10^{-6}$	c	$1{,}41 \times 10^{-6}$	c	$5{,}67 \times 10^{-7}$	d		
20	$5{,}71 \times 10^{-6}$	b			$3{,}26 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}22 \times 10^{-6}$	c	$4{,}85 \times 10^{-7}$	d		
22	$5{,}19 \times 10^{-6}$	b			$2{,}93 \times 10^{-6}$	c	$1{,}82 \times 10^{-6}$	c	$1{,}07 \times 10^{-6}$	c	$4{,}21 \times 10^{-7}$	d		
24	$4{,}76 \times 10^{-6}$	b			$2{,}65 \times 10^{-6}$	c	$1{,}62 \times 10^{-6}$	c	$9{,}47 \times 10^{-7}$	d	$3{,}70 \times 10^{-7}$	d		
27	$4{,}23 \times 10^{-6}$	b			$2{,}32 \times 10^{-6}$	c	$1{,}39 \times 10^{-6}$	c	$8{,}04 \times 10^{-7}$	d	$3{,}10 \times 10^{-7}$	d		
30			$3{,}80 \times 10^{-6}$	b	$2{,}06 \times 10^{-6}$	c	$1{,}21 \times 10^{-6}$	c	$6{,}94 \times 10^{-7}$	d	$2{,}65 \times 10^{-7}$	d	$9{,}54 \times 10^{-8}$	e
33			$3{,}46 \times 10^{-6}$	b	$1{,}85 \times 10^{-6}$	c	$1{,}06 \times 10^{-6}$	c	$5{,}94 \times 10^{-7}$	d	$2{,}30 \times 10^{-7}$	d	$8{,}57 \times 10^{-8}$	e
36			$3{,}17 \times 10^{-6}$	b	$1{,}67 \times 10^{-6}$	c	$9{,}39 \times 10^{-7}$	d	$5{,}16 \times 10^{-7}$	d	$2{,}01 \times 10^{-7}$	d	$7{,}77 \times 10^{-8}$	e
39			$2{,}93 \times 10^{-6}$	c	$1{,}53 \times 10^{-6}$	c	$8{,}40 \times 10^{-7}$	d	$4{,}53 \times 10^{-7}$	d	$1{,}78 \times 10^{-7}$	d	$7{,}11 \times 10^{-8}$	e
43			$2{,}65 \times 10^{-6}$	c	$1{,}37 \times 10^{-6}$	c	$7{,}34 \times 10^{-7}$	d	$3{,}87 \times 10^{-7}$	d	$1{,}54 \times 10^{-7}$	d	$6{,}37 \times 10^{-8}$	e
47			$2{,}43 \times 10^{-6}$	c	$1{,}24 \times 10^{-6}$	c	$6{,}49 \times 10^{-7}$	d	$3{,}35 \times 10^{-7}$	d	$1{,}34 \times 10^{-7}$	d	$5{,}76 \times 10^{-8}$	e
51			$2{,}24 \times 10^{-6}$	c	$1{,}13 \times 10^{-6}$	c	$5{,}80 \times 10^{-7}$	d	$2{,}93 \times 10^{-7}$	d	$1{,}19 \times 10^{-7}$	d	$5{,}26 \times 10^{-8}$	e
56			$2{,}04 \times 10^{-6}$	c	$1{,}02 \times 10^{-6}$	c	$5{,}10 \times 10^{-7}$	d	$2{,}52 \times 10^{-7}$	d	$1{,}03 \times 10^{-7}$	d	$4{,}73 \times 10^{-8}$	e
62			$1{,}84 \times 10^{-6}$	c	$9{,}06 \times 10^{-7}$	d	$4{,}43 \times 10^{-7}$	d	$2{,}13 \times 10^{-7}$	d	$8{,}84 \times 10^{-8}$	e	$4{,}22 \times 10^{-8}$	e
68			$1{,}68 \times 10^{-6}$	c	$8{,}17 \times 10^{-7}$	d	$3{,}90 \times 10^{-7}$	d	$1{,}84 \times 10^{-7}$	d	$7{,}68 \times 10^{-8}$	e	$3{,}80 \times 10^{-8}$	e
75			$1{,}52 \times 10^{-6}$	c	$7{,}31 \times 10^{-7}$	d	$3{,}40 \times 10^{-7}$	d	$1{,}57 \times 10^{-7}$	d	$6{,}62 \times 10^{-8}$	e	$3{,}41 \times 10^{-8}$	e
82			$1{,}39 \times 10^{-6}$	c	$6{,}61 \times 10^{-7}$	d	$3{,}01 \times 10^{-7}$	d	$1{,}35 \times 10^{-7}$	d	$5{,}79 \times 10^{-8}$	e	$3{,}08 \times 10^{-8}$	e
91			$1{,}25 \times 10^{-6}$	c	$5{,}88 \times 10^{-7}$	d	$2{,}61 \times 10^{-7}$	d	$1{,}14 \times 10^{-7}$	d	$4{,}94 \times 10^{-8}$	e	$2{,}74 \times 10^{-8}$	e
100			$1{,}14 \times 10^{-6}$	c	$5{,}28 \times 10^{-7}$	d	$2{,}29 \times 10^{-7}$	d	$1{,}01 \times 10^{-7}$	d	$4{,}29 \times 10^{-8}$	e	$2{,}47 \times 10^{-8}$	e